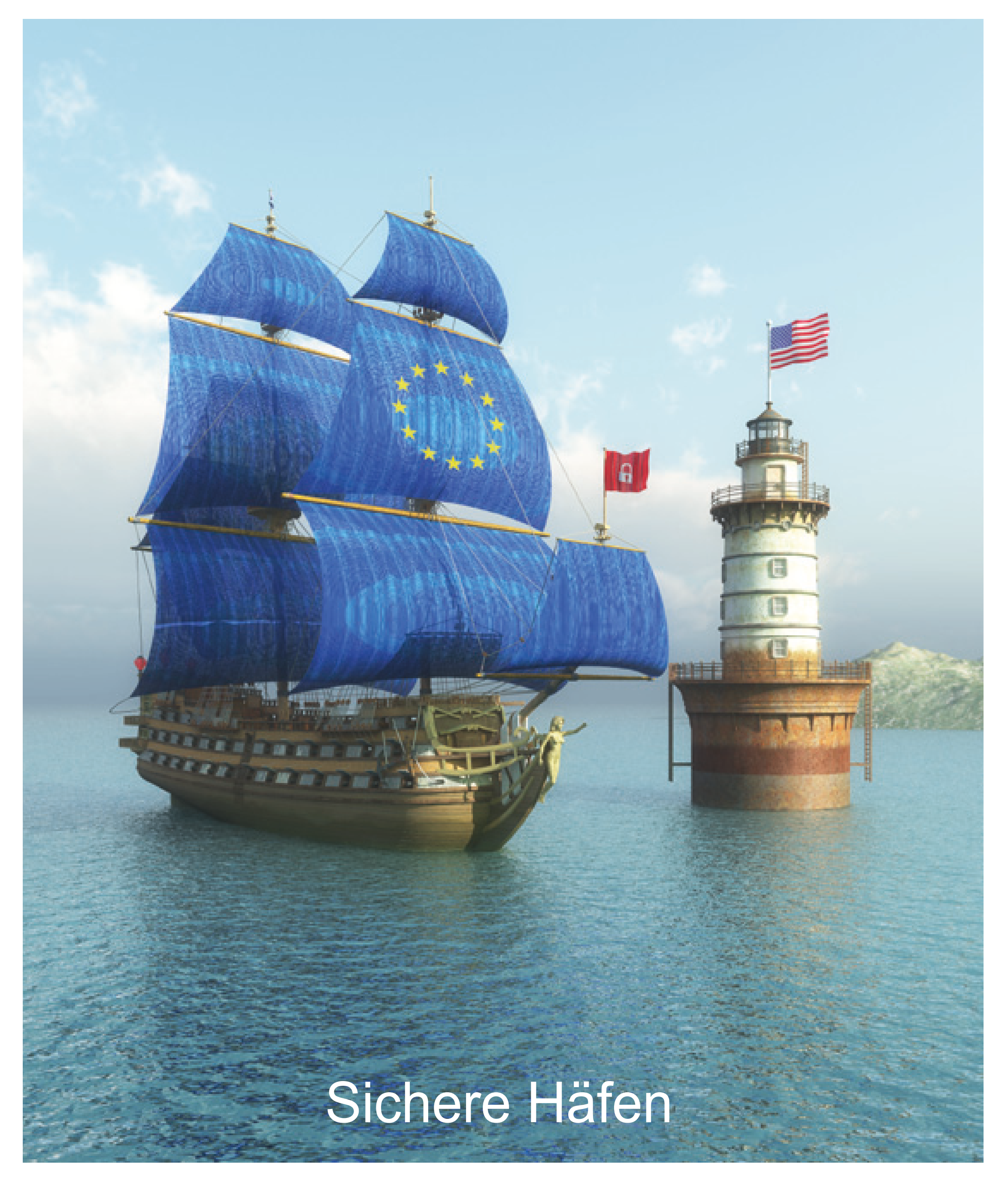
4/2015

Datenschutz Nachrichten

38. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Klarheit über die Unsicherheit des „sicheren Hafens" ■ Statements zum Safe Harbor-Urteil: ULD, Artikel-29-Datenschutzgruppe, Datenschutzbeauftragte des Bundes und der Länder ■ Mitteilung der Kommission ■ Das In-Camera-Verfahren bei den Verwaltungsgerichten ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Thilo Weichert
Klarheit über die Unsicherheit des „sicheren Hafens“ 156

Positionspapier des ULD zum Safe-Harbor-Urteil 164

Statement der Artikel-29-Datenschutzgruppe 166

Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder 167

Mitteilung der Kommission an das Europäische Parlament und den Rat 168

Pressemitteilung
Kommission: Leitlinien für transatlantische Datenübermittlungen 170

Neuer DVD-Vorstand gewählt 171

Dr. Udo Kauß
Das In-Camera-Verfahren bei den Verwaltungsgerichten 172

Werner Hülsmann
Democracy – Im Rausch der Daten 173

Datenschutz Nachrichten – Deutschland 176

Datenschutz Nachrichten – Ausland 180

Datenschutz Nachrichten – Technik 188

Rechtsprechung 190

Buchbesprechungen 197

Termine

Samstag, 16. Januar 2016
DVD-Vorstandssitzung
Berlin. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 01. Februar 2016
Redaktionsschluss DANA 1/2016
Thema: Innere Sicherheit

Freitag, 22. April 2016
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Samstag, 23. April 2016
DVD-Vorstandssitzung
Bielefeld. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Montag, 19. September 2016
ULD-Sommerakademie
Kiel
https://www.datenschutzzentrum.de/sommerakademie/

Samstag, 22. Oktober 2016
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Sonntag, 23. Oktober 2016
DVD-Mitgliederversammlung
Bonn.
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
38. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Sönke Hilbrans
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße. 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Copyright
Die Urheber- und Vervielfältigungsrechte liegen bei den Autoren. Der Nachdruck ist nach Genehmigung durch die Redaktion bei Zusendung von zwei Belegexemplaren nicht nur gestattet, sondern durchaus erwünscht, wenn auf die DANA als Quelle hingewiesen wird.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Seite 175:
Farbfilm-Verleih, Berlin

Editorial: „Safe harbors?“

Liebe Leserinnen und Leser,

die vorletzte Ausgabe unserer Datenschutznachrichten stand noch im Zeichen der Maßnahmen, mit denen Grenzbehörden und Innenverwaltungen die Spuren der Hunderttausenden, die sich auf der Flucht vor den Kriegen und Wirren im Nahen und Mittleren Ost auf den Weg nach Europa gemacht haben, verfolgen wollen. Aus Fußspuren werden Datenspuren. Eine Flut von Gesetzgebungsvorhaben mit jeweils umfangreichen datenverarbeitungsrechtlichem Beiwerk ist seitdem über den Deutschen Bundestag und über die Betroffenen gerollt. Wer hätte gedacht, dass wir alle das Bild vom sicheren Hafen so schnell auf eine andere Bedeutung scharf stellen würden?



Max Schrems bei der DVD-Datenschutzmatinée 2012 im Europaparlament in Brüssel

Mit dem Urteil des Europäischen Gerichtshofs vom 06.10.2015 hat der sympathische österreichische Aktivist Max Schrems, den wir schon bei einer DVD-Datenschutzmatinée in Brüssel und anlässlich der Verleihung der Big Brother-Awards 2015 zu unseren Gästen zählen durften, für einen wahren Urknall im europäischen Datenschutz gesorgt. Man fühlt sich fast an die Aufbruchstimmung in Bürgerrechtskreisen erinnert, welche die Kaskade datenschutzfreundlicher Entscheidungen des Bundesverfassungsgerichts in der zweiten Hälfte des letzten Jahrzehnts erzeugte. Wir widmen diese Ausgabe ausführlich dieser Entscheidung und ihren Folgen und lassen dabei auch unser altes und neues Vorstandsmitglied Dr. Thilo Weichert zu Wort kommen. Zu den Änderungen im DVD-Vorstand lesen Sie bitte ebenfalls einen Beitrag in diesem Heft.
Eine anregende Lektüre und selbstverständlich besinnliche Feiertage und einen guten Rutsch in ein gesundes, erfolgreiches und gut geschütztes Jahr 2016 wünscht Ihnen, Ihren Lieben und Ihren Daten

Sönke Hilbrans

Autorinnen und Autoren dieser Ausgabe:

Werner Hülsmann

Vorstandsmitglied in der DVD, Mitglied des Beirats des Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V., selbständiger Datenschutzberater, externer Datenschutzbeauftragter und Datenschutzsachverständiger, Ismaning und Berlin, huelsmann@datenschutzverein.de

Dr. Udo Kauß

Rechtsanwalt in Freiburg i.B., spezialisiert auf Themen der Inneren Sicherheit und des Datenschutzes. Vorsitzender des LV Baden-Württemberg der Humanistischen Union. ra@rechtsanwalt-kauss.de

Dr. Thilo Weichert

Ehemaliger Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig Holstein, Kiel, Vorstandsmitgied in der DVD, weichert@datenschutzexpertise.de

Thilo Weichert

Klarheit über die Unsicherheit des „sicheren Hafens“

Auf dem Weg zu datenschutzkonformen Datenübermittlungen in die USA

1. Einleitung

Mit Urteil vom 06.10.2015 entschied der Europäische Gerichtshof (EuGH), dass die Safe-Harbor-Entscheidung der Kommission vom 26.07.2000, wonach unter bestimmten festgelegten Voraussetzungen in den Vereinigten Staaten von Amerika (USA) ein angemessenes Datenschutzniveau zur Übermittlung personenbezogener Daten fingiert wird, ungültig ist und erklärte damit Safe Harbor für unwirksam.[1]

Damit entschied der EuGH über eine grundlegende, bisher streitige Frage des Datenschutzrechts, nämlich die Zulässigkeit von Datenübermittlung ins Drittausland, und legte Maßstäbe fest, die bisher weder Unternehmens- noch Aufsichtspraxis waren. Das Urteil führt dazu, dass europäische wie auch nationale Exekutiven und Gesetzgeber tätig werden müssen. Der vorliegende Beitrag stellt das Urteil sowie die aktuellen Reaktionen hierauf dar und zieht rechtliche praktische Schlüsse für die Zukunft.

2. Rechtliche Grundlagen

Maßstab der rechtlichen Prüfung durch den EuGH waren die europäischen Grundrechte sowie die europäische Datenschutzrichtlinie (EG-DSRl) aus dem Jahr 1995.[2]

In der seit 2009 gültigen Europäischen Grundrechte-Charta (EuGRCh) werden in den Art. 7 und 8 die Achtung des Privat- und Familienlebens sowie der Schutz personenbezogener Daten gewährleistet: Art. 7: „Jeder Mensch hat das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Kommunikation.“ Art. 8: „(1) Jeder Mensch hat das Recht auf Schutz der ihn betreffenden personenbezogenen Daten. (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jeder Mensch hat das Recht, Auskunft über die ihn betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu bewirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“ Weiterhin garantiert Art. 47 EuGRCh einen Anspruch auf wirksamen Rechtsbehelf und ein unparteiisches Gericht: „(1) Jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, hat das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen. (2) Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird. Jede Person kann sich beraten, verteidigen und vertreten lassen.“

In der europäischen Datenschutzrichtlinie (EG-DSRl) wird festgelegt, dass die Übermittlung personenbezogener Daten in ein Drittland, also in ein Land außerhalb der Europäischen Union (EU) oder des europäischen Wirtschaftsraums, grundsätzlich nur dann zulässig ist, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Gemäß Arr. 25 Abs. 6 EG-DSRl darf die Kommission feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Schutzniveau gewährleistet. Weiterhin sieht die EG-DSRl in Art. 28 Abs. 1 vor, dass jeder EU-Mitgliedstaat eine oder mehrere öffentliche Stellen benennt, die in seinem Hoheitsgebiet mit der Überwachung der Anwendung der zur Umsetzung der Richtlinie erlassenen nationalen Vorschriften beauftragt sind („Datenschutzbehörden“).

3. Der Sachverhalt

Der Kläger, der Österreicher Max Schrems. nutzt seit 2008 Facebook. Wie bei allen anderen in der Union wohnhaften Nutzern von Facebook werden seine Daten von der irischen Tochtergesellschaft von Facebook ganz oder teilweise an Server, die sich in den USA befinden, übermittelt und dort verarbeitet. Schrems legte bei der irischen Datenschutzbehörde wegen der Verarbeitung seiner Daten bei Facebook mehrere Beschwerden ein. Nach den Enthüllungen Edward Snowdens über die u. a. vom US-Geheimdienst National Security Agency (NSA) durchgeführten Überwachungs- und Kontrollaktivitäten im Internet, die auch Facebook erfassen, erweiterte Schrems seine Beschwerde und vertrat die Ansicht, dass das Recht und die Praxis in den USA keinen ausreichenden Schutz der in dieses Land übermittelten Daten vor Überwachungstätigkeiten der dortigen Behörden bieten. Die irische Behörde wies die Beschwerde insbesondere mit der Begründung zurück, die Kommission habe in ihrer Entscheidung vom 26.07.2000 festgestellt, dass im Rahmen der sogenannten „Safe-Harbor-Regelung“ ein angemessenes Datenschutzniveau für die übermittelten Daten gewährleistet sei.[3] Der auf die Klage von Schrems hiermit befasste Irish High Court hinterfragte die Wirksamkeit der Safe-Harbor-Regelung. Er machte eine Vorlage beim EuGH und wollte wissen, ob die Safe-Harbor-Entscheidung der EU-Kommission eine nationale Datenschutzbehörde daran hindert, eine Beschwerde zu prüfen, mit der geltend gemacht wird, dass ein Drittland kein an-

gemessenes Schutzniveau gewährleiste, und gegebenenfalls die angefochtene Datenübermittlung auszusetzen. Die Safe-Harbor-Regelung enthält eine Reihe von Grundsätzen über den Schutz personenbezogener Daten, denen sich amerikanische Unternehmen im Rahmen einer Selbstzertifizierung freiwillig unterwerfen können.

4. Das Urteil

Zuständiger Berichterstatter beim EuGH war der deutsche Richter Thomas von Danwitz. In seinem Urteil führt das Gericht, das als große Kammer entschied, aus, dass die Existenz einer Entscheidung der Kommission, in der festgestellt wird, dass ein Drittland ein angemessenes Schutzniveau für übermittelte personenbezogene Daten gewährleistet, die Befugnisse der nationalen Datenschutzbehörden aufgrund des Art. 8 EuGRCh weder beseitigen noch auch nur beschränken kann. Entsprechendes gelte für die den Art. 8 konkretisierende EG-DSRl. Der EuGH stellt fest, dass keine Bestimmung der EG-DSRl die nationalen Datenschutzbehörden an der Kontrolle der Übermittlungen personenbezogener Daten in Drittländer hindert, die Gegenstand einer Entscheidung der Kommission ist. Auch bei Vorliegen einer solchen EU-Kommissions-Entscheidung müssen die nationalen Datenschutzbehörden, wenn sie mit einer Beschwerde befasst werden, in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der EG-DSRl aufgestellten Anforderungen gewahrt werden.

Der EuGH weist jedoch darauf hin, dass er allein befugt ist, die Ungültigkeit eines Unionsrechtsakts wie einer Kommissions-Entscheidung festzustellen. Ist eine nationale Behörde oder die Person, die sie angerufen hat, der Auffassung, dass eine Entscheidung der Kommission ungültig ist, muss diese Behörde oder diese Person folglich die nationalen Gerichte anrufen können, damit diese, falls sie ebenfalls Zweifel an der Gültigkeit der Entscheidung der Kommission haben, die Sache dem Gerichtshof vorlegen können. Der EuGH hat letztlich darüber zu befinden, ob eine Entscheidung der Kommission gültig ist.

Der EuGH prüfte zudem die Gültigkeit der Kommissions-Entscheidung zu Safe Harbor. Er stellte fest, dass die Kommission hätte feststellen müssen, dass die USA aufgrund ihrer innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleisten, das dem in der Europäischen Union (EU) aufgrund der Richtlinie im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist. Eine solche Feststellung hatte die Kommission nicht getroffen. Sie beschränkte sich damals darauf, die Safe-Harbor-Regelung positiv zu bewerten. Der EuGH prüfte nicht, ob diese Regelung ein Schutzniveau gewährleistet, das dem in der Union garantierten Niveau der Sache nach gleichwertig ist. Er stellte vielmehr fest, dass sie nur für die amerikanischen Unternehmen gilt, die sich ihr unterwerfen, nicht aber für die Behörden der USA. Die US-Gesetze geben den Erfordernissen der nationalen Sicherheit, des öffentlichen Interesses Vorrang vor der Safe-Harbor-Regelung. US-Unternehmen sind deshalb ohne jede Einschränkung verpflichtet, die in dieser Regelung vorgesehenen Schutzregeln unangewendet zu lassen, wenn sie in Widerstreit zu solchen Erfordernissen stehen.

Die amerikanische Safe-Harbor-Regelung ermöglicht daher Eingriffe der amerikanischen Behörden in die Grundrechte der von Datenübermittlungen betroffenen Personen, ohne dass es in den USA Regeln gibt, die dazu dienen, etwaige Eingriffe zu begrenzen noch einen wirksamen gerichtlichen Rechtsschutz gegen solche Eingriffe zu gewähren. Der EuGH sah sich bei der Analyse der Regelung durch zwei Mitteilungen der Kommission bestätigt, aus denen u. a. hervorgeht, dass die amerikanischen Behörden auf die aus den Mitgliedstaaten in die USA übermittelten personenbezogenen Daten zugreifen und sie in einer Weise verarbeiten konnten, die namentlich mit den Zielsetzungen ihrer Übermittlung unvereinbar war und über das hinausging, was nach Ansicht der Kommission zum Schutz der nationalen Sicherheit absolut notwendig und verhältnismäßig gewesen wäre.[4] Desgleichen stellte die Kommission fest, dass es für die Betroffenen keine administrativen oder gerichtlichen Rechtsbehelfe gibt, die es diesen erlaubten, zu den sie betreffenden Daten Zugang zu erhalten und gegebenenfalls deren Berichtigung oder Löschung zu erwirken.

Der EuGH stellte fest, dass nach dem Unionsrecht eine Regelung nicht auf das absolut Notwendige beschränkt ist, wenn sie generell die Speicherung der personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die USA übermittelt werden, gestattet, ohne dass irgendeine Differenzierung, Einschränkung oder Ausnahme vorgenommen wird. Es fehlt an Regelungen zu den verfolgten Zielen und zu objektiven Kriterien, die es ermöglichen würden, den Zugang zu den Daten und deren spätere Nutzung zu beschränken. Eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze den Wesensgehalt des Grundrechts auf Achtung des Privatlebens. Verletzt sei außerdem der Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz, da für die Betroffenen keine Möglichkeit eröffnet ist, mittels Rechtsbehelf Zugang zu den sie betreffenden Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken. Eine solche Möglichkeit sei dem Wesen eines Rechtsstaats inhärent.

Schließlich stellte der EuGH fest, dass die Kommissions-Entscheidung zu Safe Harbor den nationalen Datenschutzbehörden die Befugnis entzieht, auf Beschwerde eines Betroffenen hin die Vereinbarkeit der Entscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte in Frage zu stellen. Gemäß dem EuGH hatte die Kommission keine Kompetenz, die Befugnisse der nationalen Datenschutzbehörden in dieser Weise zu beschränken.

Aus den vorgenannten Gründen erklärte der EuGH die Safe-Harbor-Entscheidung für ungültig. Dies hat zur Folge hat, dass die irische Datenschutzbehörde die Beschwerde von Max Schrems mit aller gebotenen Sorgfalt prüfen und am Ende der Untersuchung entscheiden muss, ob nach der EG-DS-Rl die Übermittlung der Daten europäischer Facebook-Nutzender in die USA auszusetzen ist, weil dort kein angemessenes Schutzniveau für personenbezogene Daten besteht. Es sei nun Sache der Datenschutzbehörden, über weitere

Schritte zu entscheiden. Für künftige Datenschutzabkommen behielt sich der EuGH eine strikte Kontrolle vor.

5. Erste Reaktionen

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) Andrea Voßhoff sah in dem Urteil eine erhebliche Stärkung der Datenschutzbehörden. Der in Deutschland für Facebook zuständige Hamburgische Datenschutzbeauftragte meinte, die Kritik des EuGH sei so fundamental, dass ein Stopp der Datenflusses in Betracht kommt, und: „Das ist eine späte Genugtuung für Edward Snowden." Der Verhandlungsführer des EU-Parlaments für die Europäische Datenschutz-Grundverordnung (EU-DSGVO), der Abgeordnete Jan Philipp Albrecht (Grüne) forderte, den Transfer zu unterbinden.

Vertreter der deutschen Wirtschaft verwiesen dagegen auf die laufenden Verhandlungen zwischen dem US-Handelsministerium und der EU-Kommission über eine Reform von Safe Harbor. So warnte Markus Kerber, Geschäftsführer des Bundesverbands der Deutschen Industrie (BDI): „Die USA sind Europas wichtigster Handelspartner. Ein Abbruch des Datenaustauschs wäre ein Paukenschlag".[5] In einem offenen Brandbrief an EU-Kommissionspräsident Jean-Claude Juncker forderten mehrere Wirtschaftsverbände gemeinsam eine „harmonisierte Umsetzung" des Urteils und eine „ausreichende Übergangsperiode" für Unternehmen, sich den neuen Anforderungen anzupassen.[6]

Facebook, das den Anlass für das Urteil gegeben hatte, erklärte umgehend, von diesem nicht betroffen zu sein, da man sich „wie tausende europäischer Unternehmen" auf weitere Möglichkeiten nach dem europäischen Recht verlasse, um „unabhängig von Safe Harbor" legal Daten von Europa in die USA zu übermitteln. Man könne zudem beim Registrierungsprozess vom Nutzer dessen Einverständnis einholen, womit die Übermittlung in die USA legitimiert werde.

Erstaunlich waren die Reaktionen aus der EU-Kommission. Der erste Vizepräsident der Kommission Frans Timmermans erklärte, er sehe im Urteil eine „Bestätigung für das Bestreben, den ´sicheren Hafen` neu zu verhandeln". Die Justizkommissarin Vera Jourová ergänzte, man habe seit 2013 „unnachgiebig" mit den USA an der Reform gearbeitet. Es seien „wichtige Fortschritte" erzielt worden, „auf denen wir im Lichte des Urteils aufbauen können". Bis ein neuer „sicherer Hafen" entsteht, könnten die transatlantischen Datenflüsse anhand der anderen rechtlichen Mechanismen, so Timmermans und Jourová, ungehindert weitergehen. Davon ging auch die luxemburgische Präsidentschaft in ihrem Statement aus. Der für das Digitale zuständige EU-Kommissar Günther Oettinger erklärte, dass das Urteil auch Anlass zur Selbstkritik sei: „Wir haben die Praxis in den USA jahrelang nicht konsequent genug beobachtet. … Wir müssen sehen, inwieweit sich unsere amerikanischen Partner auf unser Datenschutzniveau einlassen. Da treffen unterschiedliche Sichtweisen aufeinander. Ich warne davor, dass wir mit übertriebenen Erwartungen in die Verhandlungen gehen – und dann gar nichts erreichen. … Mich wundert immer wieder, dass wir Deutschen sehr sensibel sind, was den Datenschutz im Allgemeinen angeht".

Das EU-Parlament (EP) hatte Anfang 2014 gefordert, Safe Harbor zu überprüfen. Nach dem Urteil forderte der Vorsitzende des EP-Innenausschusses, der britische Labour-Abgeordnete Claude Moraes, „einen starken Rahmen für die Weitergabe personenbezogener Informationen" mit „soliden durchsetzbaren Datenschutzrechten und einer effektiven unabhängigen Aufsicht".[7]

In den USA wurde das EuGH-Urteil heruntergespielt. Juristen und Unternehmensvertreter meinten, die meisten großen Unternehmen könnten ihre Speicherung von Daten über Europäer in den USA auf der Basis anderer Regelungen, die vom EuGH nicht aufgehoben wurden, fortsetzen. Verwiesen wurde u. a. auf von der EU-Kommission anerkannte Standardvertragsklauseln. Außerdem wurde darauf hingewiesen, dass auch nach nationalen Sicherheitsgesetzen in Europa z. B. die Befugnis bestehe, zum Zweck der Terrorismusbekämpfung den vollständigen Internetverkehr zu scannen, wodurch ebenso massiv wie in den USA in den Datenschutz eingegriffen werde.[8]

Eine erste gerichtliche Reaktion bestand darin, dass der Irish High Court, der dem EuGH das Safe-Harbor-Thema vorgelegt hatte, am 20.10.2015 gegenüber dem Irischen Datenschutzbeauftragten anordnete, Ermittlungen wegen der Geschäftspraktiken von Facebook aufzunehmen. Der Rechtsanwalt Facebooks kündigte eine „konstruktive Mitarbeit" bei den Untersuchungen an. Der Irische Datenschutzbeauftragte kündigte an, die Schrems-Beschwerde nun „mit aller angemessenen Sorgfalt"zu prüfen.[9] Bei den deutschen Datenschutzbehörden gingen nach dem EuGH-Urteil täglich Beschwerden wegen Safe Harbor ein.

6. Behördliche Stellungnahmen

Die vom EuGH in die Pflicht gestellten Aufsichtsbehörden reagierten schnell:

6.1 Unabhängiges Landeszentrum für Datenschutz (ULD)

Als erste Aufsichtsbehörde äußerte sich umfassend das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) mit einem Positionspapier, in dem die Handlungsmöglichkeiten, genauer die Handlungspflichten von EU-Kommission und USA-Gesetzgeber, festgehalten werden: Die EU-Kommission müsse ein effektives angemessenes Datenschutzniveau von den USA fordern, wenn weiterhin ein umfassender Datenaustausch praktiziert werden soll. Letztlich sei eine umfassende Änderung des US-amerikanischen Rechts nötig. Auf der Grundlage einer Einwilligung könne eine Übermittlung in die USA nicht mehr erfolgen; denkbar sei nur die Übermittlung im Rahmen von Vertragsbeziehungen. Standardverträge seien zu kündigen; die darauf basierenden Datenübermittlungen seien auszusetzen. Das ULD wies auf seine Befugnisse hin, per verwaltungsgerichtlicher Anordnung Datenübermittlungen in die USA zu verbieten oder auszusetzen bzw. Bußgelder zu verhängen.[10] Während sich der Kläger Max Schrems in einer eigenen Stellungnahme weitgehend inhaltlich der Analyse des ULD anschloss,[11] meinte die IT-Rechtsanwältin Nina Diercks hierzu: „Es ist Wahnsinn, einfach nur Wahnsinn".[12]

6.2 Art-29-Arbeitsgruppe

Am 15.10.2015 gab die Artikel-29-Arbeitsgruppe ihr erstes Statement ab. Sie wies darauf hin, dass sie wiederholt auf die Rechtswidrigkeit der massenhaften und willkürlichen Überwachung hingewiesen habe und forderte die EU-Mitgliedstaaten und die europäischen Institutionen auf, „offene Gespräche mit den US-amerikanischen Behörden zu führen, um politische, rechtliche und technische Lösungen zu finden", damit die Grundrechte bei Übermittlungen in die USA gewahrt werden. Die aktuellen Verhandlungen für ein neues „Safe Harbor" wurden verworfen. Es bedürfe verbindlicher Mechanismen „in Bezug auf die nötige Kontrolle des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit, Rechtsmittel und Datenschutzrechte." Die Überprüfung von Standardvertragsklauseln und Binding Corporate Rules (BCRs) wurde angekündigt. Sollte bis Ende Januar 2016 keine Lösung „in Zusammenarbeit mit den US-Behörden" gefunden sein, seien die EU-Datenschutzbehörden verpflichtet, „alle notwendigen und angemessenen Maßnahmen zu ergreifen, einschließlich koordinierter Durchsetzungsmaßnahmen".[13]

6.3 Konferenz der deutschen Datenschutzbeauftragten

Am 26.10.2015 folgte ein Positionspapier der deutschen Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Dieses schließt sich in vieler Hinsicht der Artikel-29-Arbeitsgruppe an. „Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe Harbor gestützte Datenübermittlungen in die USA erhalten, werden sie diese untersagen." Die Unternehmen werden aufgefordert, „unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten". Anders als das ULD meint die Konferenz, kämen Einwilligungen „unter engen Bedingungen" als tragfähige Grundlage in Betracht. Schließlich forderte die Konferenz Kommission, Rat und Parlament der EU auf, in den laufenden Trilog-Verhandlungen dem EuGH-Urteil zu genügen.[14] In Reaktion hierauf erklärte der Industrieverband DigitalEurope, an dem Google, Apple, IBM und Nokia beteiligt sind, dass allein diese Stellungnahme schon zu einer unnötigen Wettbewerbsverunsicherung führen werde.[15]

6.4 EU-Kommission

Mit Datum vom 06.11.2015 äußerte sich die EU-Kommission erstmals mit einem offiziellen Dokument. Sie weist darauf hin, dass sie seit Januar 2014 daran arbeitet, auf der Grundlage von 13 Empfehlungen[16] Datenübertragungen für EU-Bürger sicherer zu machen. Nach dem EuGH-Urteil habe sie die Verhandlungen mit den USA intensiviert. Ziel der Kommission sei es, die Gespräche innerhalb von drei Monaten abzuschließen. In der Zwischenzeit müssten Unternehmen das Urteil befolgen und nach Möglichkeit auf alternative Datenübermittlungsinstrumente zurückgreifen. In den Leitlinien für die „Übergangszeit bis zur Annahme eines neuen Rechtsrahmens" hebt die Kommission hervor, dass das Safe-Harbor-Abkommen nicht mehr als Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA dienen kann. Bei ihren Verhandlungen mit den USA müsse die Kommission insbesondere erreichen, dass „in Bezug auf die Beschränkungen und Garantien bezüglich des Zugriffs auf personenbezogene Daten durch die US-amerikanischen Behörden" den EuGH-Anforderungen genügt wird. Darüber hinaus müssten weitere Angemessenheitsbeschlüsse geändert werden.

In der Mitteilung werden alternative Grundlagen für die Übermittlung personenbezogener Daten in die USA dargelegt, ohne der Unabhängigkeit und den Befugnissen der Datenschutzbehörden der Mitgliedstaaten bei der Rechtmäßigkeitskontrolle vorgreifen zu wollen. Datenübertragungen von Unternehmen könnten derzeit auf folgenden Grundlagen erfolgen: vertragliche Regeln, Binding Corporate Rules sowie die Ausnahmeregelungen nach Art. 26 Abs. 1 EG-DSRl. Am 15.10.2015 hatten sich EU-Vizepräsident Ansip sowie die Kommissionsmitglieder Oettinger und Jourová mit Vertretern der Unternehmen und der Industrie getroffen, wobei letztere eine klare und einheitliche Auslegung des Urteils und mehr Klarheit über die ihnen für Datenübermittlungen zur Verfügung stehenden Instrumente gefordert hatten.[17]

7. Einstufung

7.1 Der EuGH als Vorreiter

Nachdem sich der EuGH lange Zeit in Fragen des Datenschutzes eher zurückgehalten hatte, schärfte das oberste europäische Gericht in den letzten 18 Monaten sein Profil massiv. Ähnliche Paukenschlag-Entscheidungen waren das Urteil zum „Recht auf Vergessen" bei der Google-Suche[18] sowie die Ungültigkeitserklärung der EU-Richtlinie über die Vorratsspeicherung von Telekommunikationsverkehrsdaten.[19] Damit profilierte sich der EuGH als Konkurrenz und zugleich als Partner des deutschen Bundesverfassungsgerichts (BVerfG), das hinsichtlich der Präzisierung des Grundrechtes auf Datenschutzes bisher meinungsführend war. Die Rechtsprechung des EuGH gleicht teilweise bis in die Wortwahl hinein der des BVerfG, aber mit der Besonderheit, dass die Aussagen nun europaweit gelten.

7.2 Das lange Leiden mit Safe Harbor

Safe Harbor war von Anfang an ein politischer Kuhhandel ohne grundrechtliche Basis. Es ging darum, trotz des europäischen digitalen Grundrechtsschutzes, der keine Entsprechung in den USA findet, den transatlantischen Datenaustausch aufrecht zu erhalten. Angesichts der großen Bedeutung der informationellen Verflechtung zwischen den Informationswirtschaften von USA und EU sollten dem ungehinderten Profitstreben beim personenbezogenen Datenverkehr keine grundrechtlichen Hindernisse in den Weg gelegt werden.

Die Einhaltung von Safe Harbor war zunächst kein für die Öffentlichkeit relevantes Datenschutzthema. Dies änderte sich 2008 zumindest für die Fachöffentlichkeit, als Chris Connolly in seiner Galexia-Studie feststellte, dass selbst die laxen Safe-Harbor-Regeln von vielen US-Unternehmen missachtet wurden.[20] Ein Vollzug durch die US-Aufsichtsbehörde, die Federal Trade Commission (FTC) fand de facto insbesondere bei großen IT-Unternehmen nicht statt.

Trotz massiver Kritik der deutschen Datenschutzbehörden änderte sich hieran nichts grundlegend.[21] So blieb z. B. eine Beschwerde des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) wegen der Missachtung von Safe Harbor durch Facebook einfach unbeantwortet.[22]

Zum Zeitpunkt der EuGH-Entscheidung nahmen rund 4.400 Unternehmen die Erleichterungen von Safe Harbor in Anspruch, darunter sämtliche großen US-IT-Unternehmen: Google, Facebook, Microsoft, Amazon, Salesforce… Es scheint so, dass es diese Firmen sind bzw. waren, die Safe Harbor als eine mehr oder weniger lästige Pflicht abgearbeitet haben. Diesen gegenüber hatte sich – zumindest in Fragen von Safe Harbor – die US-amerikanische Aufsichtsbehörde auch als äußerst konziliant erwiesen. Dem gegenüber sollen kleinere US-amerikanische Datenimporteure die Pflichten von Safe Harbor in größerem Maße ernst genommen haben.

Das EuGH-Urteil kam also nicht überraschend. Die von Unternehmen vergossenen Krokodilstränen entwichen Reptilien, die sich jahrelang unter Missachtung der datenschutzrechtlichen Regeln den Bauch vollgehauen haben. Nachdem sich schon die EU-Kommission kritisch zu Safe Harbor geäußert und das Votum des Generalanwalts im EuGH-Verfahren an Safe Harbor nichts Gutes gelassen hatte, war nur noch fraglich, wie deutlich und mit welcher Begründung der EuGH Safe Harbor verwerfen würde. Der EuGH hat sich in seiner Begründung im Umfang beschränkt, aber die wesentlichen Knackpunkte mit einer kaum zu übertreffenden Klarheit herausgearbeitet.

Zum Zeitpunkt des EuGH-Urteils verhandelte die EU-Kommission mit den USA seit zwei Jahren über eine Neuregelung von Safe Harbor. Die geheimen Gespräche sollen kurz vor einem Abschluss gestanden haben, wobei – soweit dies bekannt ist – bisher nur eher kosmetische Korrekturen konsentiert waren. Diese dürften in vieler Hinsicht den geleakten Vereinbarungen zu einem Umbrella-Abkommen für Datenübermittlungen zum Zweck der Strafverfolgung entsprochen haben (s. u. 9.2). Das US-Außenministerium hatte noch kurz vor dem EuGH-Urteilsspruch beteuert, das NSA-Überwachungsprogramm Prism richte sich gegen „konkrete zulässige Ziele“. Ein Aus von Safe Harbor würde dem Schutz der Bürgerrechte „erheblichen Schaden“ zufügen und den „freien Fluss von Informationen verhindern.[23]

8. Konsequenzen

Den Stellungnahmen der Aufsichtsbehörden zu den Folgewirkungen ist zuzustimmen: Mit dem Urteil ist ab sofort die Rechtfertigung von Datentransfers in die USA per Safe Harbor nicht mehr möglich. Interessanterweise bleibt Safe Harbor als Selbstverpflichtung nach US-amerikanischem Recht dort weiter wirksam.

Die Ausführungen des EuGH gelten nicht nur für Safe Harbor, sondern umfassend auch für Standardvertragsklauseln, Binding Corporate Rules (BCRs) sowie für die Datenweitergabe öffentlicher Stellen, etwa bei Übermittlungen für Zwecke der Terrorismusbekämpfung und für andere Zwecke der öffentlichen Sicherheit und der Strafverfolgung.

8.1 Standardvertragsklauseln

Die Urteilsgründe sind insofern unmissverständlich, dass die aktuellen Standardvertragsklauseln keine rechtliche Basis mehr haben. Wie die Datenschutzaufsichtsbehörden richtig feststellten, beschränkt sich die Wirkung des EuGH-Urteils nicht auf Safe Harbor. Unternehmensanwälte und sogar die EU-Kommission gaben den Ratschlag, auf dieses Instrument nunmehr auszuweichen. Dies wurde von vielen Unternehmen dann auch tatsächlich umgehend umgesetzt. Um diese nicht in falscher Sicherheit zu wiegen, sollte die EU-Kommission – statt Nebelkerzen abzubrennen – ihre Beschlüsse zu den Standarvertragsklauseln umgehend aufheben und durch neue Regelwerke ersetzen (s. u. 8.9).

8.2 Europäische Datenverarbeitung

Die wirksamste und für die Unternehmen wie für die Betroffenen sicherste Reaktion auf das Urteil ist es, dass die verantwortlichen Stellen ihre bisher in den USA erfolgende Datenverarbeitung nach Europa holen. Dann besteht ein geringeres Risiko der Massenüberwachung ohne Rechtsschutzmöglichkeiten für die Betroffenen. Dies gilt auch für Konzerne und Unternehmensgruppen mit Teilen in den USA. US-Behörden können zwar über den Patriot Act, den Foreign Intelligence Surveillance Act (FISA) wie über weitere US-rechtliche Instrumente in Europa gespeicherte Daten einfordern.[24] Hiergegen können sich die Unternehmen aber tatsächlich und rechtlich zur Wehr setzen, so wie dies – bisher ohne Erfolg – Microsoft in einem konkreten Fall versucht.[25] Werden mit den USA verflochtene Unternehmen in eine Datenverarbeitung einbezogen, so sollte in den entsprechenden Verträgen verpflichtend eine Information über entsprechende Herausgabeforderungen vorgesehen werden, die auch an die eigenen Aufsichtsbehörden und die Betroffenen weitergegeben werden kann. Dies steht zwar regelmäßig im Widerspruch zu US-Recht. Derartige Konflikte zwischen verschiedenen Pflichten aus verschiedenen Rechtskreisen sind nichts Ungewöhnliches – gerade für international tätige Unternehmen. Über das mit diesen Konflikten verbundene Risiko sollten sich die beteiligten Stellen bewusst sein.

8.3 Massenüberwachung auch in Europa

Eine interessante Frage ist, inwieweit das EuGH-Urteil Übermittlungen in das United Kingdom (UK) ausschließt, wo – wie in den USA – durch den britischen Geheimdienst GCHQ anlasslose Massenüberwachungsmaßnahmen praktiziert werden. Inzwischen wissen wir, dass derartige Maßnahmen nicht nur von Diensten im UK durchgeführt werden, sondern auch vom deutschen Bundesnachrichtendienst sowie anderen europäischen Diensten. In Frankreich sollen derartige flächendeckende Überwachungsmaßnahmen gerade per Gesetz legalisiert werden.[26]

Bei einer Verarbeitung innerhalb der EU ist die Rechtslage zumindest insofern klar: Wegen des normativ gewährleisteten Datenschutzniveaus im Empfängerland darf – dem europäischen

Binnenmarkt und der europäischen Datenschutzrichtlinie (EG-DSRl) sei Dank – keine Datentransfer verweigert werden. Im Konfliktfall kann – u. a. unter Berufung auf Art. 7, 8 und 47 EuGRCh – Rechtsschutz erlangt werden.

8.4 Freihandelsabkommen?

Die Hoffnungen, über Freihandelsabkommen, etwa das transatlantische Abkommen zwischen der EU und den USA (TTIP), aus der Grundrechtsbindung von grenzüberschreitenden Datentransfers ausbrechen zu können, sind unbegründet. Diese Abkommen enthalten regelmäßig gemäß Art. 14 GATT im Hinblick auf den Datenschutz eine Ausnahmeklausel. Dessen ungeachtet ist darauf zu achten, dass diese Generalausnahme nicht durch spezifische Regelungen faktisch ausgehebelt werden[27].

8.5 Binding Corporate Rules

Die Entscheidung der deutschen Datenschutzbehörden, zunächst keine BCRs mehr nach § 4c Abs. 2 Bundesdatenschutzgesetz (BDSG) zu genehmigen, ist konsequent. Die bestehenden BCRs dürften weitgehend nicht den materiell-rechtlichen Anforderungen des EuGH genügen. Nach entsprechender Anerkennung durch die Aufsichtsbehörden in der Vergangenheit entfalten diese aber weiterhin eine rechtliche Wirkung. Angesichts der nun vorliegenden klarstellenden EuGH-Rechtsprechung fehlte den bisher erfolgten Genehmigungen nach heutiger Erkenntnis die materiell-rechtliche Grundlage. Die erfolgt jeweils auf der Basis eines von Anfang an rechtswidrigen Verwaltungsaktes. Die Aufsichtsbehörden sind aufgefordert, zunächst generell neue Anforderungen an BCRs zu formulieren, diese den Unternehmen mitzuteilen und zu verlangen, ihre BCRs innerhalb einer angemessenen Frist anzupassen. Wird dem nicht entsprochen, so können die Genehmigungen nach dem jeweiligen Verwaltungsverfahrensrecht (vgl. § 48 BVwVfG) zurückgenommen werden. Hinsichtlich der Anforderungen kann auf die Ausführungen zu den Standardvertragsklauseln verwiesen werden (s. u. 8.9).

8.6 Übergangsfrist?

Die offiziellen Stellen – also auch die Aufsichtsbehörden – dürfen die Unternehmen nicht längere Zeit im Ungewissen lassen, aber auch nicht überfordern. Insofern ist die von der Artikel-29-Arbeitsgruppe gesetzte Frist vom 31.01.2016 als Stillhaltezusage in Bezug auf konkrete Sanktionen zu begrüßen. Diese entbindet die Aufsichtsbehörden aber nicht, umgehend die betroffenen Unternehmen zu kontaktieren und Lösungen einzufordern. Die mit der Fristsetzung explizit verbundene Erwartung im Hinblick auf die US-Position ist aber illusorisch: Auch wenn die EU-Kommission dies von den USA einfordern wird, so werden sich nach den bisherigen Erfahrungen diese weigern, den Anforderungen des EuGH an einen gerichtlichen Rechtsschutz, materielle Datenschutzrechte und eine Umsetzung des Verhältnismäßigkeitsgrundsatzes nachzukommen. Erfolgversprechender ist der Ansatz, zeitnah die Standardvertragsklauseln an das EuGH-Urteil anzupassen (dazu näher unter 8.9). Dazu sollte die EU-Kommission bis Ende Januar 2016 in der Lage sein.

8.7 Rechtsgrundlage Einwilligung

Bevor der rechtlich geforderte Mindestinhalt von Standardvertragsklauseln und BCRs erörtert wird, ist auf die kontrovers erörterte Frage einzugehen, inwieweit Einwilligungen Datentransfers in die USA rechtfertigen können. Insofern weist das ULD zurecht darauf hin, dass vor Einholung einer wirksamen Einwilligung nachweisbar auf das fehlende Datenschutzniveau und auf die US-staatlichen Zugriffsbefugnisse hingewiesen werden muss, um zumindest ansatzweise zu gewährleisten, dass die erteilte Einwilligung informiert erfolgte. Der formularmäßige Hinweis in allgemeinen Geschäftsbedingungen (AGB) genügt nicht. Sind alle weiteren Anforderungen an eine wirksame Einwilligung – insbesondere Freiwilligkeit, Information über die Art der Daten, die Zwecke und die verarbeitenden Stellen – gegeben, so können Einwilligungen wirksam sein. Hinsichtlich von Einwilligungen in Beschäftigungsverhältnissen ist die Freiwilligkeit nur gegeben, wenn der Beschäftigte ohne berufliche Nachteile zu befürchten diese verweigern kann.

8.8 Rechtsgrundlage: Vertrag mit dem Betroffenen

Dem ULD ist auch zuzustimmen, dass Übermittlungen zur Vertragserfüllung zulässig sein können. Da trotz der umfassenden Berichterstattung in den Medien der Mangel des Datenschutzniveaus in den USA nicht als allgemein bekannt vorausgesetzt werden kann, ist es – im Interesse der Wirksamkeit der erfolgenden Willenserklärung bei Vertragsabschluss – dringend zu empfehlen und wohl in den meisten Fällen rechtlich gefordert, in dem Vertragstext einen expliziten Hinweis auf das bestehende Risiko zu geben. Um keine Missverständnisse entstehen zu lassen: Vertragsbasierte Datenübermittlungen setzen Verträge zwischen dem Betroffenen und verarbeitenden Stellen voraus; Drittdaten können auf dieser Grundlage nicht weitergegeben werden.

8.9. Vertragliche Verpflichtung des Datenexporteurs

Es ist wohl realistisch, dass zumindest mittelfristig in den USA die anlasslose massenhafte Internetüberwachung nicht eingestellt wird und dass es auch nicht zu einer gesetzlichen Anerkennung eines einklagbaren, dem europäischen Grundrecht auf Datenschutz vergleichbaren Anspruchs von Jedermann auf Datenschutzrechte kommen wird. So stellt sich die Frage: Wie können Stellen in Europa den Anforderungen des EuGH genügen, wenn Übermittlungen absolut unvermeidlich sind? Wie kann ein angemessener Ausgleich zwischen der Achtung des Grundrechts auf Privatsphäre und den Interessen an einen freien Verkehr personenbezogener Daten aussehen?[28]

Insofern dürfte – außer bei direkter Betroffenenbeteiligung (s.o. 8.7 u. 8.8), also insbesondere bei Standardvertragsklauseln und BCRs – mittelfristig nur ein Weg gangbar sein: Der Datenexporteur verpflichtet den Datenimporteur, abgesichert durch hinreichende Sanktionen wie Vertragsstrafen und Haftungsübernahmen – vergleichbar der Auf-

tragsdatenverarbeitung – im Einzelfall umfassend Auskunft über die dort erfolgende Datenverarbeitung zu geben. Diese Auskunft ermöglicht es dem Exporteur, Auskunft an den Betroffenen oder an die für ihn zuständige Aufsichtsbehörde zu geben. Über den Datenexporteur müssen alle dort geltenden gesetzlichen Betroffenenrechte geltend gemacht werden können, die mangels Rechtsschutz in den USA dort nicht administrativ und gerichtlich durchgesetzt werden können. Zu den Betroffenenrechten gehört auch das Recht, eine unabhängige Datenschutzaufsichtsbehörde anzurufen, die dann die Rechtmäßigkeit der Datenübermittlung im konkreten Einzelfall überprüfen kann. Im Rahmen dieser Prüfung muss und kann sie dann auch ermitteln, ob der Datenimporteur seinen vertraglichen Pflichten und Garantien entspricht bzw. entsprochen hat.[29] Ist der Betroffenen der Ansicht, dass seine Datenschutzrechte verletzt werden, so kann er auch unter Berufung auf diesen Vertrag den Rechtsweg gegen den Datenexporteur beschreiten.[30] Um diese Möglichkeit zu eröffnen, muss der Exporteur seinen Transfervertrag zugunsten der Drittbetroffenen entweder veröffentlichen oder in anderer geeigneter Weise die Betroffenen hierüber informieren.

9. Weitere Folgewirkungen

9.1 Trilog

Das EuGH-Urteil hat Auswirkungen auf die Trilog-Verhandlungen zwischen Kommission, Parlament und Rat der EU zu einer Europäischen Datenschutz-Grundverordnung (EU-DSGVO). Es ist zu hoffen und unabdingbar, dass die Normen zu grenzüberschreitenden Datenübermittlungen in der EU-DSGVO mit den grundrechtlich abgeleiteten Anforderungen des EuGH in Einklang stehen. Entsprechendes gilt auch für die ebenso im Trilog verhandelte Datenschutzrichtlinie für die Bereiche Innen und Justiz. Das Erfordernis eines angemessenen – nicht identischen – Datenschutzes in den Empfängerländern gilt schon derzeit in der EG-DSRl. Wünschenswert ist, dass der europäische Gesetzgeber gemäß den materiellen Anforderungen des EuGH explizite Prüfkriterien für die Angemessenheit des Datenschutzniveaus im Empfängerland normiert.

9.2 Umbrella-Abkommen

Keine Zukunftsperspektive hat das weitgehend ausverhandelte Umbrella-Abkommen zwischen der EU und den USA zur Datenübermittlung zum Zweck der Strafverfolgung.[31]

9.3 Fluggast- und Bankdatenabkommen

Die EU-Justizkommissarin Vera Jourová vertrat die Ansicht, dass das EuGH-Urteil zu Safe Harbor keine Auswirkungen auf den Flug- und Bankdatentransfer habe, also auf die Übermittlungen von Passenger Name Records (PNR) und von Daten des internationalen Bankdienstleisters SWIFT im Rahmen des Terrorist Finance Tracking Programs (TFTP). Sie begründet dies damit, dass dort der Zugriff der US-Behörden an enge Vorgaben geknüpft sei und den EU-Bürgern überdies die Möglichkeit eingeräumt sei, sich per Verwaltungs- oder gerichtlicher Verfahren gegen ungerechtfertigte Zugriffe zu wehren.[32] Diese Äußerung zeugt von einem in einem Rechtsstaat nicht zu tolerierenden Primat der Politik (s.u. 10). Frau Jourová ist nicht entgangen, dass die theoretisch zulässigen Rechtsmittel keine Wirksamkeit entfalten. Diese basieren auf einem leicht zu erkennenden Umstand: der Verweigerung der grundrechtlich geforderten Datentransparenz, ohne die jegliches Rechtsschutzbegehren ins Leere läuft.

9.4 Geheimdienste

Die Diskussion, inwieweit sich das EuGH-Urteil auf die anlasslose Datenerhebung und den Datenaustausch zwischen nationalen Geheimdiensten – auch innerhalb der EU – auswirkt, hat erst begonnen und muss intensiv geführt werden.

9.5 Facebook-Verfahren vor dem BVerwG

Die grünen Landtagsabgeordneten Burkhard Peters und Rasmus Andresen wiesen darauf hin, dass das EuGH-Urteil Einfluss auf die ausstehende Entscheidung des Bundesverwaltungsgerichts (BVerwG) im Rechtsstreit zwischen dem ULD und den Betreibern von Facebook-Fanpages im Lande haben wird, worüber am 25.02.2016 verhandelt wird. Das zentrale Argument des ULD, dass das Betreiben einer Fanpage ein rechtlich und technisch einheitlicher Vorgang ist, bei dem Fanpage-Betreiber und Facebook sich gegenseitig ergänzen und voreinander abhängig sind, werde gestützt. Der Betrieb von Facebook-Fanpages verstoße, wie der EuGH klargestellt hat, massiv gegen deutsches und europäisches Datenschutzrecht.[33]

9.6 Klagerecht der Datenschutzaufsichtsbehörden

Angesichts der gewaltigen Bedeutung des EuGH-Urteils für den grenzüberschreitenden Datenverkehr ist eine Erwägung des EuGH bisher wenig diskutiert worden, die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Stellungnahme vom 26.10. unter Punkt 11 kurz und knapp thematisiert wurde: „Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.“[34]

10. Abschlussbemerkungen

Das vorliegende EuGH-Urteil wird noch oft besprochen, diskutiert, kommentiert und zitiert werden. Die sich hieraus ergebenden politischen und rechtlichen Konsequenzen sollten darin bestehen, dass das mit der Safe-Harbor-Entscheidung der EU-Kommission im Jahr 2000 zum Ausdruck gebrachte unsägliche Primat der Politik beim internationalen Datenschutz dem „Rule of Law“, also der Herrschaft des Rechts, weicht. Safe Harbor beruhte von Anfang an auf der Überlegung, wirtschaftliche Erwägungen, die Macht des Faktischen und die freundschaftlichen Beziehungen zu den USA über die Rechtsstaatlichkeit zu stellen.

Erschreckend sind die ersten Signale von EU-Rat und EU-Kommission, wonach die Lektion bisher nicht verstanden wurde und keine klare Umkehr erfolgen soll. Beim Datenschutz gibt es einen vergleichbaren Dauerkonflikt zwischen dem deutschen Gesetzgeber und dem Bundesverfassungsgericht insbesondere in Sicherheitsfragen, der schon zu vielen

Gerichtsurteilen gegen Bundesgesetze geführt hat, nicht aber zu einer verfassungskonformen Selbstbeschränkung des Gesetzgebers. Der Bundesgesetzgeber hat soeben mit seinem Gesetz zur Vorratsdatenspeicherung von Telekommunikationsdaten seine Maßlosigkeit erneut unter Beweis gestellt. Ein klügeres, weniger arbeits- und energieaufwändigeres Prozedere auf europäischer Ebene wäre wünschenswert – ist aber wohl nicht realistisch.

Ein Bekenntnis zu einem grundrechtskonformen gelebten Datenschutz läge auch im Interesse der europäischen IT-Wirtschaft. Die Umsetzung des EuGH-Urteils eröffnet für diese die Chance, zumindest auf dem europäischen Markt nicht mehr deshalb benachteiligt zu sein, weil sie sich – anders als viele große US-Unternehmen – effektiv an Recht und Gesetz orientieren. Ein beliebtes Argument der offiziellen US-Seite in diesem Konflikt ist, dass die Grundrechtsorientierung und der damit einher gehende europäische „Daten-Nationalismus“ nicht nur in einer globalen Informationsgesellschaft anachronistisch, sondern auch nichts anderes als ethisch verpackter Protektionismus sei. Selbst wenn es das wäre: Die USA verhält sich ebenso, wenn sie den chinesischen Technologiekonzern Huawei von öffentlichen Aufträgen ausschließt.[35]

Die gleichbehandelnde Anwendung des Grundrechtsschutzes der Bürger bei europäischen wie bei US-Unternehmen könnte außerdem den Effekt haben, dass die US-Wirtschaft Druck auf die US-Administration ausübt, endlich auch in den USA digitalen Grundrechtsschutz zu etablieren, der nicht nur für US- und evtl. für EU-Bürger gilt, sondern für alle Menschen. So unwahrscheinlich es derzeit erscheinen mag, es muss das Bestreben dahin gehen, mit Hilfe des EuGH-Urteils zu Safe Harbor die USA – eingeschlossen die dortige Regierung und den Supreme Court – dazu zu bringen, sich seiner verloren gegangenen freiheitlichen und demokratischen Ursprünge zu besinnen und diese den Umständen unserer hochtechnisierten Informationsgesellschaft und unserer modernen Zeit anzupassen und fortzuentwickeln.

1 EuGH, U. v. 06.10.2015, C-362/14, abzurufen unter http://curia.europa.eu/juris/liste.jsf? td=ALL&language=de&jur=C,T,F&num=C-362/14.

2 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, S. 31.

3 Entscheidung 2000/520/EG der Kommission vom 26.07.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufg gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215, S. 7.

4 Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel „Wiederherstellung des Vertrauens beim Datenaustausch zwischen der EU und den USA“, COM[2013] 846 fnal, 27.11.2013, und Mitteilung der Kommission an das Europäische Parlament und den Rat über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen, COM[2013] 847 fnal, 27.11.2013.

5 Janisch, Historisches Urteil zum Datenschutz, SZ 07.10.2015, 1.

6 EU-Datenschützer setzen Ultimatum für Safe Harbor 2.0, www.heise.de 17.10.2015.

7 Krempl, Safe Harbor: EU-Kommission sieht nach EuGH-Urteil keinen Grund, Datenfüsse zu stoppen, www.heise.de 07.10.2015; Interview von Müller mit Oetinger, „Anlass zur Selbstkritk“, Der Spiegel 42/2015, 45.

8 Mass Surveillance, The New York Times Internatonal Weekly, SZ 16.10.2015, 2.

9 Humphries, Irish court orders investgaton of Facebook data transfer to U.S., www.reuters.com 20.10.2015.

10 Positonspapier des ULD zum Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14 v. 14.10.2015, https://www.datenschutzzentrum.de/artkel/967-.html.

11 Vgl. http://www.europe-v-facebook.org/EN/Complaints/PRISM/Response/response.html#alts.

12 Diercks, Safe Harbor, www.socialmediarecht.de 14.10.2015.

13 Vgl. http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/StatementOfTheArticle29WorkingParty.html?cms_templateQueryString=article+29+working+party&cms_sortOrder=score+desc.

14 http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.html?cms_submit=Senden&cms_templateQueryString=safe+harbor+update+positionspapier.

15 Stupp, Tech Industry associaton bashes German privacy watchdogs, www.euractiv.com, 28.10.2015.

16 Communicaton from the Commission to the European Parliament and the Council on the Functoning of the Safe Harbour from the Perspectve of EU Citzens and Companies Established in the EU, 27.11.2013, COM(2013) 847 fnal.

17 Communicaton from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directve 95/46/EC following the Judgment by the Court of Justce in Case C-362/14 (Schrems), 6.11.2015, COM(2015) 566 fnal; PM Europäische Kommission v. 06.11.2015, Kommission veröfentlicht Leitlinien für transatlantsche Datenübermitlungen und fordert rasche Einigung auf neuen Rechtsrahmen als Konsequenz aus dem Schrems-Urteil.

18 EuGH, U. v. 13.05.2014, C-131/12, AfP2014, 245.

19 EuGH, U. v. 08.04.214, C-293/12, C-594/12, NVwZ 2014, 709.

20 Zusammenfassend Chris Connolly, EU/US Safe Harbor–Efectveness of the Framework in relation to Natonal Security Surveillance, http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf.

21 Vgl. ULD, PE v. 23.07.2010; 10 Jahre Safe Harbor – viele Gründe zum Handeln, kein Grund zum Feiern, https://www.datenschutzzentrum.de/presse/20100723-safe-harbor.htm.

22 Schreiben des ULD an die FTC vom 21.08.2012, https://www.datenschutzzentrum.de/uploads/facebook/20120821-ftc-facebook-de.pdf.

23 Hurtz, Sicherer Server gesucht, SZ 07.10.2015, S. 2.

24 ULD, https://www.datenschutzzentrum.de/internationales/20111115-patriot-act.html.

25 Bernau/Seeling, Grenzüberschreitung, SZ 22.01.2015, 19.

26 Ermert, Überwachung: Frankreichs Senat winkt Carte Blanche für Geheimdienst durch, www.heise.de 28.10.2015.

27 Weichert, Freihandelsabkommen contra Datenschutz? DuD 2014, 850

28 EuGH, U. v. 06.10.2015, C-362, Rn. 42.

29 EuGH, U. v. 06.10.2015, C-362, Rn. 47, 57.

30 EuGH, U. v. 06.10.2015, C-362, Rn. 64.

31 Kritsch schon zuvor Schaar, Leaky Umbrella, 18.09.2015, http://www.eaid-berlin.de/?p=779; Korff, EU-US Umbrella Data Protecton Agreement, 14.10.2015, http://free-group.eu/2015/10/14/eu-us-umbrella-data-protection-agreement-detailed-analysis-by-douwe-korff/; Boehm, A Comparison between US and EU data protecton legislaton for law enforcement puposes, 2015, S. 71 f., http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU%282015%29536459_EN.pdf.

32 Ermert, EU-Kommissarin: Safe Harbor ohne Auswirkung auf Flug-und Bankdatentransfer, www.heise.de 27.10.2015.

33 PE vom 06.10.2015 Nr. 408.15, Das heutge EuGH-Urteil wird auch Auswirkungen auf den Rechtsstreit des ULD gegen Fanpagebetreiber haben!

34 EuGH, U. v. 06.10.2015, Rn. 65.

35 Zand, Das digitale Chinatown, Der Spiegel 44/2015, 102.

Positionspapier des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zum Safe-Harbor-Urteil des Gerichtshofs der Europäischen Union vom 6. Oktober 2015, C-362/14

Dieses Positionspapier richtet sich an nichtöffentliche und öffentliche Stellen in ihrer Funktion als verantwortliche Stellen für Datenverarbeitungen (§ 3 Abs. 7 BDSG/§ 2 Abs. 3 LDSG) und soll verdeutlichen, welche Folgen das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein aus dem „Safe-Harbor-Urteil“ des Gerichtshofs der Europäischen Union (EuGH) vom 06.10.2015, C-362/14, zieht.

Zunächst wird dargestellt, welche Aussagen der EuGH in seinem Urteil getroffen bzw. nicht getroffen hat (1). Das Positionspapier nimmt danach Stellung zu der Frage, welche Handlungsoptionen nach dem Urteil für die EU-Kommission bestehen (2), auf Basis welcher Rechtsgrundlagen eine Übermittlung personenbezogener Daten in die USA noch in Betracht kommt bzw. nicht mehr zulässig ist (3) und wie mit den Standardvertragsklauseln umzugehen ist (4). Schließlich wird dargestellt, welche Auswirkungen die gerichtliche Entscheidung – soweit dies derzeit absehbar ist – auf die Prüftätigkeit des ULD hat (5).

1. Inhalt des Urteils

Der EuGH hat die Safe-Harbor-Entscheidung der Europäischen Kommission für ungültig erklärt. Während die darin geregelte Selbstzertifizierung US-amerikanischer Unternehmen bisher als Grundlage für Datenübermittlungen in die USA herangezogen wurde, ist dies mit Verkündung des Urteils nicht mehr zulässig.

Allem voran nimmt der EuGH Bezug auf Mitteilungen der Kommission an das Europäische Parlament und den Rat aus November 2013, in denen die Kommission diverse Schutzlücken ihrer Safe-Harbor-Entscheidung darstellt. Mit Blick auf diese Feststellungen der Kommission selbst macht der EuGH in seinem Urteil deutlich, dass die Safe-Harbor-Entscheidung ungültig ist, weil sie keine ausreichende Begrenzung der Zugriffe von staatlichen Behörden bewirke. Ebenso fehle es in der Safe-Harbor-Entscheidung an jeder Feststellung über ausreichende Rechtsschutzmöglichkeiten für europäische Bürgerinnen und Bürger. Ohne das Rechtssystem der USA konkret zu bewerten, stellt der EuGH abstrakt fest, dass nationale Regelungen, die es generell gestatten, auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Grundrechts auf Achtung des Privatlebens verletzen.

Zudem schränke die Safe-Harbor-Entscheidung die Aufsichtsbefugnisse der europäischen Datenschutz-Aufsichtsbehörden zu sehr ein und halte sich nicht an die Vorgaben, auf Basis derer die Kommission über das Schutzniveau eines Drittstaates entscheiden könne. Statt wie es Art. 25 Abs. 6 der Richtlinie 95/46/EG verlangt, habe die Kommission keine Aussage über das Datenschutzniveau in den USA getroffen, sondern mit den Safe-Harbor-Grundsätzen eine untaugliche Hilfskonstruktion als Ersatz für das unangemessene Schutzniveau gewählt.

Der EuGH hat damit nicht abschließend über das in den USA geltende Schutzniveau geurteilt, sondern das Verfahren zur Klärung dieser konkreten Fragen an das irische Ausgangsgericht zurücküberwiesen.

2. Handlungsmöglichkeiten der EU-Kommission

a) Die Kommission könnte auf Basis von Art. 25 Abs. 6 der Richtlinie 95/46/EG eine neue Entscheidung erlassen, in der sie feststellt, dass die USA ein angemessenes Schutzniveau bieten. Hierzu wäre u.a. das Folgende zu beachten:

Das datenschutzrechtliche Schutzniveau in den USA für die Freiheiten und Grundrechte der Betroffenen muss nach den Vorgaben des EuGH im Licht der Grundrechtecharta dem europäischen Schutzniveau gleichwertig sein. Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben die Enthüllungen von Edward Snowden offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen und damit die Safe-Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden. Die USA können deshalb keine innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen vorweisen, die ein angemessenes Schutzniveau bieten.

Nach den Vorgaben des EuGH erfordert die Annahme eines angemessenen Schutzniveaus einen wirksamen gerichtlichen Rechtsschutz für europäische Bürgerinnen und Bürger gegen Eingriffe in das Grundrecht auf Achtung der Privatsphäre. Es darf kein genereller Zugriff der staatlichen US-Behörden auf elektronische Kommunikation erfolgen, da dies gegen den Wesensgehalt von Art. 7 der Grundrechtecharta verstoßen würde. Haben EU-Bürgerinnen und -Bürger keine Möglichkeit, Zugang zu ihren personenbezogenen Daten zu erlangen bzw. gerichtlichen Rechtsschutz in Anspruch zu nehmen, läge ein Verstoß gegen Art. 47 der Grundrechtecharta vor.

Bei der Prüfung des angemessenen Datenschutzniveaus müsste die Kommission auf bestehende sowie gesetzlich flankierte Schutzmechanismen und Regulierungsinstrumente in den USA abstellen und diese einer Adäquanzprüfung unterziehen. Ein von der Kommission selbst entwickeltes Regulierungsinstrument wie die Safe-Harbor-Grundsätze sind vor diesem Hintergrund nicht tragfähig und würden diesen Anforderungen nicht im Ansatz genügen.

b) Die Kommission könnte einen völkerrechtlichen Vertrag wie etwa ein Datenschutzabkommen mit den USA forcieren. Dieser völkerrechtliche Vertrag müsste insbesondere die Anforderungen der Art. 7, 8 Abs. 1 und 47 Abs. 1 der Grundrechtecharta erfüllen. Auch hierzu müssten die USA zunächst die inländische Datenverarbeitung gesetzlich regeln und dabei vor allem den generellen und zweckfreien Zugriff auf den Inhalt der elektronischen Kommunikation einstellen und einen wirksamen gerichtlichen Rechtsschutz für die EU-Bürgerinnen und Bürger vorsehen. Nach den Vorgaben des EuGH müssen ausreichende Garantien zum Schutz der Grundfreiheiten/Grundrechte der EU-Bürgerinnen und Bürger gerade im Hinblick auf die automatisierte Datenverarbeitung hin vorgesehen werden.

Ergebnis: Eine Entscheidung der Kommission zur Angemessenheit des Datenschutzniveaus in den USA erfordert ebenso wie der Abschluss eines völkerrechtlichen Datenschutzabkommens eine umfassende Änderung US-amerikanischen Rechts. Da entsprechende Änderungen derzeit nicht zu erwarten sind, scheiden beide Handlungsoptionen kurz- oder mittelfristig aus.

3. Rechtsgrundlagen für die Übermittlung personenbezogener Daten

Die Übermittlung personenbezogener Daten in Länder, in denen kein angemessenes Datenschutzniveau besteht, muss für nichtöffentliche Stellen anhand von § 4c Abs. 1 des Bundesdatenschutzgesetzes (BDSG), für öffentliche Stellen in Schleswig-Holstein nach § 16 Abs. 2 des Landesdatenschutzgesetzes (LDSG) beurteilt werden. Dabei ergeben sich für den Datentransfer in die USA folgende Leitlinien:

a) § 4c Abs. 1 Nr. 1 BDSG und § 16 Abs. 2 Satz 2 Nr. 1 LDSG legitimieren eine Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau auf Basis einer Einwilligung des Betroffenen. Die Einwilligung muss „ohne jeden Zweifel" gegeben werden, Art. 26 Abs. 1 Buchstabe a der Richtlinie 95/46/EG, Art. 29-Datenschutzgruppe, WP 187, S. 32. Eine wirksame Einwilligungserklärung erfordert nicht nur eine Aufklärung über die Zwecke, sondern auch über die Risiken der Datenverarbeitung bzw. den damit verbundenen Verzicht auf ein gleichwertiges bzw. angemessenes Schutzniveau. Der Betroffene müsste daher zunächst umfassend über das fehlende Schutzniveau, vor allem über US-staatliche Zugriffsbefugnisse, fehlende Rechtsschutzmöglichkeiten/Betroffenenrechte, Weiterverarbeitung der Daten ohne Zweckgebundenheit, die Nichtgeltung des Erforderlichkeitsgrundsatzes sowie über fehlende staatliche Kontrollmechanismen in den USA aufgeklärt werden.

Für die Wirksamkeit einer Einwilligungserklärung muss insbesondere immer eine Aufklärung über die konkreten Zwecke der Verarbeitung erfolgen, § 4a Abs. 1 Satz 2 BDSG. Schließlich wäre für die Einwilligung erforderlich, dass eine Erklärung „für den konkreten Fall" bzw. für eine konkrete Datenverarbeitung abgegeben wird, Art. 29-Datenschutzgruppe, WP 187, S. 20 ff. Eine Generalerklärung für eine Vielzahl von nicht übersehbaren Datenverarbeitungen wird regelmäßig unzulässig sein. Speziell in Beschäftigungsverhältnissen würde den Beschäftigten hinsichtlich ihrer Erklärungen auch keine Wahlfreiheit verbleiben, soweit der Arbeitgeber eine Einwilligung für die Übermittlung ihrer personenbezogenen Daten in die USA verlangt. Es würde keine freie Entscheidung im Sinne von § 4a Abs. 1 BDSG, § 12 Abs. 2 LDSG vorliegen und damit keine wirksame Erklärung. Sehen US-amerikanische Vorschriften eine nicht zweckgebundene Datenverarbeitung durch staatliche Behörden vor, so scheitert bereits hieran die wirksame Einwilligung.

Selbst bei ausreichender Information über die Risiken und auch in Fällen, in denen noch von einer Freiwilligkeit ausgegangen werden könnte, würde die Einwilligung grundsätzlichen Bedenken begegnen. Die anlasslose Massenüberwachung durch Geheimdienste greift nach Ansicht des EuGH in den Wesensgehalt des Grundrechts auf Achtung des Privatlebens ein. Derartige Eingriffe sind nach bundesverfassungsgerichtlicher Rechtsprechung jedoch der Disposition des Einzelnen, auch im Wege einer Einwilligung, entzogen. Dies kann sich auch auf die Einwilligung in die Datenübermittlung in einen Staat erstrecken, in dem der Wesensgehalt der Grundrechte der EU nicht gewahrt wird. Die Aufnahme einer solchen Einwilligung etwa in Allgemeine Geschäftsbedingungen wäre mit größter Wahrscheinlichkeit sittenwidrig im Sinne des § 138 BGB.

Ergebnis: Die Einwilligung nach § 4a BDSG, § 12 LDSG scheidet nach den obigen Ausführungen als Rechtsgrundlage für die Zulässigkeit der Übermittlung trotz fehlenden angemessenen Datenschutzniveaus aus.

b) Im Bereich der Privatwirtschaft kommen als Rechtsgrundlagen im Wesentlichen nur § 4c Abs. 1 Nr. 2 und 3 BDSG in Betracht. Demnach ist die Datenübermittlung zulässig für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, soweit dies erforderlich ist, § 4c Abs. 1 Nr. 2 BDSG. Erfasst sind hiervon etwa Reise- und Flugbuchungen. Weiterhin wäre die Datenübermittlung zulässig, sofern diese zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll, § 4c Abs. 1 Nr. 3 BDSG. Beide Tatbestände bilden jedoch keine Übermittlungsgrundlagen für Beschäftigtendaten, welche in den USA z.B. zur Leistungs- oder Verhaltenskontrolle verarbeitet werden.

4. Umgang mit Standardvertragsklauseln durch nichtöffentliche Stellen

Exemplarisch wird auf Klausel 5 Buchstabe b des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittstaaten vom 5. Februar 2010 (2010/87/EU) verwiesen. Demnach garantiert der Datenimporteur gegenüber dem europäischen Datenexporteur unter anderem, dass er seines Wissens keinen Gesetzen unterliegt, die ihm die Befolgung der Anweisungen des Datenexporteurs und die Einhaltung seiner vertraglichen Pflichten unmöglich machen. Genau diese vertragliche Pflicht können US-amerikanische Vertragspartner mit Blick auf das in den USA geltende Recht aber nicht einhalten. Der Datenexporteur ist in derartigen Fällen berechtigt, die Datenübermittlung auszusetzen oder den Standardvertrag zu kündigen. Gleiches gilt z.B. nach Klausel 5 Buchstabe b des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittstaaten vom 27. Dezember 2001 (2002/16/EG) und nach Klausel 5 Buchstabe a des Beschlusses der Kommission über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittstaaten vom 15. Juni 2001 (2001/497/EG).

Ergebnis: Nichtöffentliche Stellen, die für ihren Datentransfer in die USA Standardvertragsklauseln verwenden, müssen nun in Erwägung ziehen, den zugrunde liegenden Standardvertrag mit dem Datenimporteur in den USA zu kündigen oder die Datenübermittlungen auszusetzen. In konsequenter Anwendung der Vorgaben des EuGH in seinem Urteil ist eine Datenübermittlung auf Basis von Standardvertragsklauseln nicht mehr zulässig.

5. Prüftätigkeit des ULD gegenüber nichtöffentlichen Stellen

a) Im Bereich der Standardvertragsklauseln – exemplarisch Art. 4 Buchstabe a des Beschlusses der Kommission vom 5. Februar 2010 (2010/87/EU) – können die Aufsichtsbehörden Datenübermittlungen in die USA per verwaltungsrechtlicher Anordnung verbieten oder aussetzen. Die Anordnung ist möglich, wenn der Datenimporteur oder Unterauftragsverarbeiter nach den geltenden US-Vorschriften sich nicht an europäisches Datenschutzrecht/die Vorgaben der Standardvertragsklauseln halten können und die Anforderungen nach Art. 13 der Richtlinie 95/46/EG erfüllt sind. Die Datenexporteure aus Europa können dies nur abwenden, indem sie von ihrem vertraglich bestehenden Recht Gebrauch machen, den Standardvertrag mit dem US-Datenimporteur aufzukündigen (exemplarisch Klausel 5 b des Beschlusses der Kommission vom 5. Februar 2010 – 2010/87/EU).

b) Die Übermittlung personenbezogener Daten in die USA ohne Rechtsgrundlage erfüllt den Bußgeldtatbestand nach § 43 Abs. 2 Nr. 1 BDSG und kann mit einem Bußgeld in Höhe von bis zu 300.000 € geahndet werden.

Ergebnis: Das ULD wird prüfen, ob Anordnungen gegenüber nichtöffentlichen Stellen getroffen werden müssen, auf deren Basis Datenübermittlungen in die USA ausgesetzt oder verboten werden müssen. Ferner ist zu prüfen, ob nichtöffentliche Stellen infolge der Datenübermittlung in ein Drittland mit fehlendem angemessenem Datenschutzniveau Ordnungswidrigkeiten verwirklicht haben.

Dieses Dokument ist im Internet zu finden unter https://www.datenschutzzentrum.de/artikel/967-.html

Statement der Artikel-29-Datenschutzgruppe

Brüssel, 16. Oktober 2015

Im Anschluss an die Grundsatzentscheidung des Gerichtshofs der Europäischen Union (EuGH) vom 6. Oktober 2015 in der Rechtssache Maximilian Schrems gegen Data Protection Commissioner (C-362/14) haben die an der Artikel-29-Datenschutzgruppe beteiligten EU-Datenschutzbehörden über die ersten Konsequenzen diskutiert, die auf europäischer und nationaler Ebene zu ziehen sind. Die EU-Datenschutzbehörden sind der Auffassung, dass ein starker gemeinsamer Standpunkt zur Umsetzung des Urteils von elementarer Bedeutung ist. Zudem wird die Datenschutzgruppe genau verfolgen, wie sich die vor dem irischen High Court anhängigen Verfahren entwickeln.

Zunächst betont die Datenschutzgruppe, dass die Frage der massenhaften und willkürlichen Überwachung ein zentrales Element in der Analyse des Gerichtshofs ist. Sie erinnert daran, dass sie wiederholt darauf hingewiesen hat, dass eine derartige Überwachung nicht mit EU-Recht vereinbar ist und dass die bestehenden Übermittlungsinstrumente in diesem Fall keine Lösung darstellen. Wie bereits erwähnt, gelten Übermittlungen an Drittstaaten, in denen die Befugnisse staatlicher Stellen beim Zugriff auf Informationen über das in einer demokratischen Gesellschaft angemessene Maß hinausgehen, zudem nicht als Übermittlungen in sichere Zielstaaten. In diesem Zusammenhang ist es durch das EuGH-Urteil erforderlich, dass jede Angemessenheitsentscheidung auch eine weitreichende Analyse der innerstaatlichen Rechtsvorschriften und internationalen Verpflichtungen des Drittstaats enthält.

Die Datenschutzgruppe fordert daher die Mitgliedstaaten und die europäischen Institutionen nachdrücklich dazu auf, offene Gespräche mit den US-amerikanischen Behörden zu führen, um politische, rechtliche und technische Lösungen zu finden, damit die Grundrechte bei Datenübermittlungen in das Hoheitsgebiet der Vereinigten Staaten gewahrt werden. Solche Lösungen könnten durch Verhandlungen in einem zwischenstaatlichen Abkommen gefunden werden, das Betroffenen in der EU stärkere Garantien bietet. Die derzeitigen Verhandlungen über ein neues „Safe Harbour" könnten Teil der Lösung sein. Auf jeden Fall sollten diese Lösungen stets mit klaren und verbindlichen Mechanismen einhergehen und zumindest Verpflichtungen in Bezug auf die nötige Kontrolle des staatlichen Zugriffs, Transparenz, Verhältnismäßigkeit, Rechtsmittel und Datenschutzrechte enthalten.

In der Zwischenzeit wird die Datenschutzgruppe weiter untersuchen, wie sich das EuGH-Urteil auf andere Übermittlungsinstrumente auswirkt. Die Datenschutzbehörden gehen während dieser Zeit davon aus, dass die Standardvertragsklauseln und BCR weiter verwendet werden können. Dies wird die Datenschutzbehörden jedoch nicht davon abhalten, bestimmte Fälle zu untersuchen, zum Beispiel auf der Grundlage von Beschwerden, und ihre Befugnisse zum Schutz von Einzelpersonen auszuüben.

Falls bis Ende Januar 2016 noch keine angemessene Lösung in Zusammenarbeit mit den US-amerikanischen Behörden gefunden wurde und je nachdem, wie die Einschätzung der Datenschutzgruppe zu den Übermittlungsinstrumenten aussieht, sind die EU-Datenschutzbehörden verpflichtet, alle notwendigen und angemessen Maßnahmen zu ergreifen, einschließlich koordinierter Durchsetzungsmaßnahmen.

Hinsichtlich der praktischen Konsequenzen des EuGH-Urteils ist die Datenschutzgruppe der Ansicht, dass Übermittlungen aus der Europäischen Union in die Vereinigten Staaten nicht mehr auf der Grundlage der Angemessenheitsentscheidung der Europäischen Kommission 2000/250/EG („Safe-Harbour-Entscheidung") erfolgen können. In jedem Fall sind Übermittlungen, die nach dem EuGH-Urteil auf der Grundlage der Safe-Harbour-Entscheidung erfolgen, rechtswidrig.

Um sicherzustellen, dass alle Beteiligten ausreichend informiert werden, werden die EU-Datenschutzbehörden auf nationaler Ebene angemessene Informationskampagnen ins Leben rufen. Dabei können beispielsweise alle Unternehmen, die die Safe-Harbour-Entscheidung angewandt haben, direkt informiert und allgemeine Mitteilungen auf den Internetseiten der Behörden eingestellt werden.

Abschließend lässt sich sagen, dass die Datenschutzgruppe darauf beharrt, dass Datenschutzbehörden, EU-Institutionen, Mitgliedstaaten und Unternehmen gemeinsam dafür verantwortlich sind, nachhaltige Lösungen für die Umsetzung des EuGH-Urteils zu finden. Insbesondere sollten Unternehmen im Kontext des Urteils über die Risiken nachdenken, die sie bei der Datenübermittlung letztendlich eingehen, und die rechtzeitige Einführung rechtlicher und technischer Lösungen in Erwägung ziehen, um diese Risiken zu minimieren und den EU-Datenschutz-Acquis einzuhalten.

Quelle: http://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2015/22_SafeHarborIstGekippt_WasNun.html?nn=5217154

Positionspapier der Datenschutzkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.10.2015

1. Nach dem Safe-Harbor-Urteil des EuGH vom 6. Oktober 2015 ist eine Datenübermittlung aufgrund der Safe-Harbor-Entscheidung der Kommission vom 26. Juli 2000 (2000/520/EG) nicht zulässig.

2. Im Lichte des Urteils des EuGH ist auch die Zulässigkeit der Datentransfers in die USA auf der Grundlage der anderen hierfür eingesetzten Instrumente, etwa Standardvertragsklauseln oder verbindliche Unternehmensregelungen (BCR), in Frage gestellt.

3. Der EuGH stellt fest, dass die Datenschutzbehörden der EU-Mitgliedstaaten ungeachtet von Kommissions-Entscheidungen nicht gehindert sind, in völliger Unabhängigkeit die Angemes-

senheit des Datenschutzniveaus in Drittstaaten zu beurteilen.

4. Der EuGH fordert die Kommission und die Datenschutzbehörden auf, das Datenschutzniveau in den USA und anderen Drittstaaten (Rechtslage und Rechtspraxis) zu untersuchen und gibt hierfür einen konkreten Prüfmaßstab mit strengen inhaltlichen Anforderungen vor.

5. Soweit Datenschutzbehörden Kenntnis über ausschließlich auf Safe-Harbor gestützte Datenübermittlungen in die USA erlangen, werden sie diese untersagen.

6. Die Datenschutzbehörden werden bei Ausübung ihrer Prüfbefugnisse nach Art. 4 der jeweiligen Kommissionsentscheidungen zu den Standardvertragsklauseln vom 27. Dezember 2004 (2004/915/EG) und vom 5. Februar 2010 (2010/87/EU) die vom EuGH formulierten Grundsätze, insbesondere die Randnummern 94 und 95 des Urteils, zugrunde legen.

7. Die Datenschutzbehörden werden derzeit keine neuen Genehmigungen für Datenübermittlungen in die USA auf Grundlage von verbindlichen Unternehmensregelungen (BCR) oder Datenexportverträgen erteilen.

8. Unternehmen sind daher aufgerufen, unverzüglich ihre Verfahren zum Datentransfer datenschutzgerecht zu gestalten. Unternehmen, die Daten in die USA oder andere Drittländer exportieren wollen, sollten sich dabei auch an der Entschließung der DSK vom 27.03.2014 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und an der Orientierungshilfe „Cloud Computing“ vom 09.10.2014 orientieren.

9. Eine Einwilligung zum Transfer personenbezogener Daten kann unter engen Bedingungen eine tragfähige Grundlage sein. Grundsätzlich darf der Datentransfer jedoch nicht wiederholt, massenhaft oder routinemäßig erfolgen.

10. Beim Export von Beschäftigtendaten oder wenn gleichzeitig auch Daten Dritter betroffen sind, kann die Einwilligung nur in Ausnahmefällen eine zulässige Grundlage für eine Datenübermittlung in die USA sein.

11. Die Datenschutzbehörden fordern die Gesetzgeber auf, entsprechend dem Urteil des EuGH den Datenschutzbehörden ein Klagerecht einzuräumen.

12. Die Kommission wird aufgefordert, in ihren Verhandlungen mit den USA auf die Schaffung ausreichend weitreichender Garantien zum Schutz der Privatsphäre zu drängen. Dies betrifft insbesondere das Recht auf gerichtlichen Rechtsschutz, die materiellen Datenschutzrechte und den Grundsatz der Verhältnismäßigkeit. Ferner gilt es, zeitnah die Entscheidungen zu den Standardvertragsklauseln an die in dem EuGH-Urteil gemachten Vorgaben anzupassen. Insoweit begrüßt die DSK die von der Art. 29-Gruppe gesetzte Frist bis zum 31. Januar 2016.

13. Die DSK fordert die Bundesregierung auf, in direkten Verhandlungen mit der US-Regierung ebenfalls auf die Einhaltung eines angemessenen Grundrechtsstandards hinsichtlich Privatsphäre und Datenschutz zu drängen.

14. Die DSK fordert Kommission, Rat und Parlament auf, in den laufenden Trilog-Verhandlungen die strengen Kriterien des EuGH-Urteils in Kapitel V der Datenschutzgrundverordnung umfassend zur Geltung zu bringen.

Quelle: http://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art-29Gruppe/Safe-Harbor_Update%2026_10_2015_Positionspapier%20DSK.html?nn=5217154

Mitteilung der Kommission an das Europäische Parlament und den Rat

über den Transfer von Personendaten von der EU in die Vereinigten Staaten von Amerika (USA) gemäß Richtlinie 95/46/EG in Reaktion auf das Urteil des Europäischen Gerichtshofs im Fall C-362/14 (Schrems)

Brüssel, 06.11.2015, COM(2015) 566/endg.

… 2.3 Ausnahmen

In Ermangelung einer Angemessenheitsentscheidung nach Art. 25 Abs. 6 Richtlinie 95/46/EG und ungeachtet der Anwendung von Standardvertragsklauseln (SCC) und/oder Binding Corporate Rules (BCR), können Personendaten an Stellen mit Sitz in einem Drittland immer noch transferiert werden, soweit eine der alternativen Ausnahmen in Art. 26 Abs. 1 Richtlinie 95/46/EG anwendbar ist:

a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder

b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder

c) die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder

d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder

e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder

f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

Diese Gründe liefern Ausnahmen zum generellen Verbot des Transfers persönlicher Daten an Stellen mit Sitz in Drittländern ohne angemessenes Schutzniveau. Tatsächlich muss der Datenexporteur in diesen Fällen nicht sicherstellen, dass der Datenimporteur einen angemessenen Schutz gewährleistet, und er benötigt regelmäßig auch keine vorhergehende Erlaubnis für den Transfer von den zuständigen Behörden. Dessen ungeachtet müssen diese Ausnahmen nach Ansicht der Artikel-29-Arbeitsgruppe eng ausgelegt werden. …

3. Die Konsequenzen des Schrems-Urteils auf Angemessenheitsentscheidungen

… Die Reichweite des Urteils ist beschränkt auf die Kommissionsentscheidung zu Safe Habor. Doch enthält jede der anderen Angemessenheitsentscheidungen eine Begrenzung der Kompetenzen der Datenschutzbehörden, wie sie auch in Art. 3 der Safe-Harbor-Entscheidung enthalten ist und die der Gerichtshof für unwirksam erklärt hat. Die Kommission wird nun die nötigen Konsequenzen aus dem Urteil ziehen, indem kurzfristig eine Entscheidung vorbereitet wird, die im anwendbaren Kommitologie-Verfahren angenommen werden soll und mit der diese Regelung in allen bestehenden Angemessenheitsentscheidungen ersetzt wird.

4. Schlussfolgerung

Wie von der Artikel-29-Arbeitsgruppe bestätigt wurde, können alternative Instrumente zur Zulassung von Datenflüssen weiterhin von Unternehmen für zulässige Datentransfers in Drittstaaten wie die USA genutzt werden. Doch hält die Kommission weiterhin einen erneuerten und robusten Rahmen für Transfers in die USA für eine prioritäre Schlüsselaufgabe. Ein solcher Rahmen wäre die umfassendste Lösung zur Sicherstellung einer wirksamen Fortsetzung des Schutzes persönlicher Daten von EU-Bürgern bei einem Transfer in die USA. Er wäre auch die beste Lösung für transatlantischen Handel, da er einen einfacheren, weniger aufwändigen und deshalb kostengünstigeren Transfermechanismus insbesondere für kleinere und mittlere Unternehmen (KMU) bieten würde.

Die Kommission hat schon 2013 mit der US-Regierung auf der Basis seiner 13 Empfehlungen Verhandlungen über ein neues Regelwerk für transatlantische Datentransfers begonnen. Es gab dabei beträchtliche Fortschritte, die Sichtweisen beider Seiten zusammenzubringen, etwa bzgl. der Überwachung und Durchsetzung der Safe-Harbor-Datenschutz-Grundsätze durch das US-Handelsministerium bzw. die Federal Trade Commission (US-FTC), mehr Verbrauchertransparenz über deren Datenschutzrechte, einfachere und billigere Abhilfemöglichkeiten im Fall von Beschwerden und klareren Regeln bei der Datenweiterübermittlung von Safe-Harbor-Unternehmen an Unternehmen außerhalb von Safe Harbor (z. B. für Zwecke der Unterauftragsdatenverarbeitung). Nachdem nun die Safe-Harbor-Entscheidung für unwirksam erklärt worden ist, hat die Kommission die Gespräche mit der US-Regierung intensiviert, um den Anforderungen zu genügen, die der Gerichtshof formuliert hat. Das Ziel der Kommission ist es, diese Diskussionen innerhalb von drei Monaten abzuschließen und dieses Ziel zu erreichen.

Bis dahin, also bis ein überarbeiteter transatlantischer Rahmen geschaffen ist, müssen sich die Unternehmen auf verfügbare alternative Transferinstrumente verlassen können. Doch bringt diese Option Verantwortlichkeiten für die unter der Aufsicht der Datenschutzbehörden stehenden Datenexporteure mit sich.

Im Gegensatz dazu, dass die Kommission die Angemessenheit des Datenschutzniveaus eines Drittstaates festgestellt hat, worauf sich ein Datenexporteur beim Datentransfer aus der EU verlassen kann, bleibt Letztgenannter dafür verantwortlich, dass die Personendaten effektiv mit den alternativen Instrumenten geschützt werden. Dies mag nötige angemessene zusätzliche Maßnahmen nötig machen.

Internet-Fundstelle für die gesamten Leitlinien in englischer Sprache: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf
Übersetzung: Thilo Weichert



Kommission veröffentlicht Leitlinien für transatlantische Datenübermittlungen und fordert rasche Einigung auf neuen Rechtsrahmen als Konsequenz aus dem Schrems-Urteil

Brüssel, 16. Oktober 2015

Der Europäische Gerichtshof hatte in seinem Urteil vom 6. Oktober in der Rechtssache Schrems die Bedeutung des Grundrechts auf Datenschutz insbesondere bei der Übermittlung personenbezogener Daten in Drittländer unterstrichen.

Die Europäische Kommission arbeitet seit Januar 2014 daran, auf der Grundlage von 13 Empfehlungen Datenübertragungen für EU-Bürger sicherer zu machen. Im Anschluss an das Urteil des Gerichtshofes hat die Kommission die Verhandlungen mit den Vereinigten Staaten über einen neuen und sicheren Rahmen für die Übermittlung personenbezogener Daten intensiviert. Ziel der Kommission ist es, die Gespräche innerhalb von drei Monaten abzuschließen.

In der Zwischenzeit müssen Unternehmen das Urteil befolgen und nach Möglichkeit auf alternative Datenübermittlungsinstrumente zurückgreifen. Wie bereits vom ersten Vizepräsidenten Timmermans und von Kommissionsmitglied Jourová am Tage des Urteilsspruches angekündigt, hat die Kommission heute Leitlinien für die Übergangszeit bis zur Annahme eines neuen Rechtsrahmens veröffentlicht. In der betreffenden Mitteilung der Kommission werden die Folgen des Urteils analysiert und alternative Verfahren für die Übermittlung von personenbezogenen Daten in die Vereinigten Staaten erörtert. Die Kommission wird zudem weiterhin eng mit den unabhängigen Datenschutzbehörden zusammenarbeiten, um eine einheitliche Umsetzung des Urteils sicherzustellen.

Vizepräsident Andrus Ansip (zuständig für den digitalen Binnenmarkt) sagte dazu: „Wir brauchen ein Abkommen mit unseren US-amerikanischen Partnern in den nächsten drei Monaten. Die Kommission ist aufgefordert worden, rasch zu handeln, und genau das werden wir tun. Wir legen heute klare Leitlinien vor, und wir setzen uns einen festen zeitlichen Rahmen für den Abschluss der Verhandlungen. Die EU und die Vereinigten Staaten sind der wichtigste Handelspartner füreinander. Datenströme zwischen unseren Kontinenten sind von wesentlicher Bedeutung für Menschen und Unternehmen. Auch wenn es alternative Möglichkeiten gibt, ist ein sicherer neuer Rahmen doch die beste Lösung für den Schutz unserer Bürger und zum Bürokratieabbau für Unternehmen und insbesondere für junge Unternehmen.“

Kommissionsmitglied Vera Jourová ergänzte: „ Die Bürger brauchen robuste Garantien für den Schutz ihrer Grundrechte, und die Unternehmen brauchen Klarheit in dieser Zwischenzeit. Deshalb möchten wir heute erläutern, unter welchen Bedingungen Unternehmen auf rechtmäßige Art und Weise vorübergehend Daten übermitteln können. Wir werden auch weiterhin eng mit den nationalen Datenschutzbehörden zusammenarbeiten, die für die Durchsetzung der Datenschutzvorschriften in den Mitgliedstaaten verantwortlich sind. Ich habe die laufenden Gespräche mit den Vereinigten Staaten über einen neuen und soliden Rahmen für transatlantische Datenübermittlungen intensiviert und werde die Gespräche nächste Woche in Washington fortführen. Ein etwaiges neues Abkommen muss die Bestimmungen des EuGH-Urteils erfüllen.”

In der Mitteilung hebt die Kommission folgende Punkte hervor:

- Das Safe-Harbor-Abkommen kann nicht mehr als Rechtsgrundlage für die Übermittlung personenbezogener Daten in die Vereinigten Staaten dienen.
- Die Kommission wird die Verhandlungen über einen neuen und soliden Rahmen fürtransatlantische Übermittlungen personenbezogener Daten fortsetzen und zum Abschluss bringen, wobei dieser Rahmen die Anforderungen des Urteils erfüllen muss, insbesondere in Bezug auf die Beschränkungen und Garantien bezüglich des Zugriffs auf personenbezogene Daten durch die US-amerikanischen Behörden,
- Darüber hinaus werden weitere Angemessenheitsbeschlüsse geändert werden müssen, damit die Datenschutzbehörden der Mitgliedstaaten auch künftig Beschwerden von Einzelpersonen ungehindert nachgehen können.

In der Mitteilung werden alternative Grundlagen für die Übermittlung personenbezogener Daten in die Vereinigten Staaten dargelegt, ohne der Unabhängigkeit und den Befugnissen der Datenschutzbehörden der Mitgliedstaaten zur Prüfung der Rechtmäßigkeit einer solchen Datenübermittlung vorzugreifen. Datenübertragungen von Unternehmen können derzeit auf folgenden Grundlagen erfolgen:

- **Vertragliche Regeln:** Vertragliche Regeln müssen bestimmte Pflichten (z.B. Sicherheitsmaßnahmen, Benachrichtigung der betroffenen Person, Sicherheitsvorkehrungen bei der Übermittlung sensibler Daten usw.) vorsehen. Mustervertragsklauseln sind hier verfügbar.
- **Verbindliche unternehmensinterne Vorschriften für unternehmensgruppeninterne Datenübermittlungen:** Auf der Grundlage derartiger Vorschriften können personenbezogene Daten unbegrenzt zwischen den Unternehmen einer weltweit operierenden Unternehmensgruppe übermittelt werden. Die Übermittlungen bedürfen jeweils der Zustimmung der Datenschutzbehörde des Mitgliedstaats, aus dem das multinationale Unternehmen Daten übermitteln möchte.

- **Ausnahmeregelungen:**
  - Datenübermittlung zum Abschluss oder zur Erfüllung eines Vertrags [einschließlich vorvertraglicher Situationen, beispielsweise zur Buchung eines Flugs oder eines Hotelzimmers in den Vereinigten Staaten];
  - Durchsetzung oder Verteidigung von Rechtsansprüchen;
  - (falls kein anderer Grund besteht:) Datenübermittlung bei aus freien Stücken und in voller Sachkenntnis erfolgender Zustimmung der betroffenen Person.

Hintergrund

Der Europäische Gerichtshof hat in seinem Urteil vom 6. Oktober in der Rechtssache Schrems die SafeHarbor-Entscheidung der Kommission für ungültig erklärt. Durch das Urteil wurden die seit November 2013 unternommenen Bemühungen der Kommission um eine Überarbeitung des Safe-Harbor-Abkommens mit dem Ziel eines nach EU-Recht hinreichenden Datenschutzes bestätigt.

Am 15. Oktober trafen Vizepräsident Ansip sowie die Kommissionsmitglieder Öttinger und Jourová mit Vertretern der Unternehmen und der Industrie zusammen. Dabei forderten letztere eine klare und einheitliche Auslegung des Urteils und mehr Klarheit über die ihnen für Datenübermittlungen zur Verfügung stehenden Instrumente.

Am 16. Oktober veröffentlichten die 28 Datenschutzbehörden der Mitgliedstaaten (Artikel-29Datenschutzgruppe) eine Erklärung über die Folgen des Urteils.

Weitere Informationen:
MEMO/15/6014

Neuer DVD-Vorstand gewählt

Das Jahr 2014 endete für den DVD-Vorstand bekanntlich etwas holprig, nachdem unsere langjährige Vorstandsvorsitzende Karin Schuler und auch unser Beisitzer Karsten Neumann aus dem Vorstand zurückgetreten waren. Karin Schuler hat ihre persönlichen Gründe dazu auch in einer Mitgliedernachricht erläutert. Mit dem vom Vorstand daraufhin neu gewählten Vorsitzenden Sönke Hilbrans und mit Frank Spaeing als neuem stellvertretenden Vorsitzenden haben wir das für den ganzen Vorstand arbeitsreiche Datenschutzjahr 2014/2015 bewältigt. Höhepunkte waren dabei der Umzug in eine neue Geschäftsstelle und die Planung einer fulminanten Jahrestagung. Dass wir diese letztlich im Oktober nicht durchführen konnten, bedauern wir noch heute sehr. Weder die viele notwendige Organisationsarbeit, noch dieser Rückschlag haben uns allerdings im ausgehenden Jahr davon abgehalten, uns als Vorstand neu aufzustellen:

So traten bei der Mitgliederversammlung am 11. Oktober 2015 in Bonn neue Kandidatinnen und Kandidaten für die zu besetzenden Vorstandsämter an und wurden gewählt: Frank Spaeing (Halle/Saale) tritt nach einem Jahr als Stellvertreter nunmehr die Nachfolge von Sönke Hilbrans (Berlin) als Vorsitzender an. Er ist freiberuflicher Datenschutzberater und gehört dem Vorstand seit 2013 an. Frank Spaeing betreut seit Jahren die Website der DVD und ist zugleich langjähriges Mitglied im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.. Stellvertreterin des Vorsitzenden und Kassiererin ist Jaqueline Rüdiger (Dortmund), die hauptberuflich mit dem Datenschutz in der Datenschutzabteilung eines großen Energieversorgers befasst ist. Auch Jaqueline Rüdiger, die sich schon zuvor in der DVD engagiert hatte, gehört dem Vorstand seit 2013 an. Sie übernimmt von dem durch Zeitablauf aus dem Vorstand ausgeschiedenen Kassenwart Robert Colombara intakte Vereinsfinanzen und hat ihren Vorgänger schon im Laufe des ausgehenden Jahres unterstützt. Mit Werner Hülsmann (Ismaning) ist ein erfahrener freiberuflicher Datenschutzberater und Aktivist ebenfalls zum stellvertretenden Vorsitzenden gewählt worden. Werner Hülsmann hatte in der Vergangenheit bereits dem DVD-Vorstand als Beisitzer angehört gehabt, war Mitglied in der Jury der Big Brother Awards und engagiert sich auch beim AK Vorrat, im FiFF und vertritt die DVD bei EDRi. Neben dem DANA-Layouter und Künstler Frans Valenta (Bonn), welcher in den Vorstand wiedergewählt wurde, und dem FORBIT-Geschäftsführer Reinhard Linz (Bonn) verstärkt neuerdings auch wieder unser langjähriger ehemaliger Vorsitzender Dr. Thilo Weichert (Kiel) als Beisitzer den Vorstand. Sönke Hilbrans wurde ebenfalls als Beisitzer in den Vorstand gewählt. Wir freuen uns ganz besonders darüber, dass Thilo Weichert nach Jahren einer zugegebenermaßen ebenfalls nicht ganz unbedeutenden Rolle in der deutschen Datenschutzlandschaft wieder zurück in den ehrenamtlichen Datenschutz gefunden hat. Sie können es schon dieser Ausgabe der DANA anmerken.

Das neue Vorstandsteam ist damit nicht mehr so rheinisch besetzt wie in den Jahren zuvor und hat auch schon seine erste, außerordentliche Vorstandssitzung in Dortmund abgehalten. Wir treffen uns als Vorstand (wozu Sie als Mitglieder herzlich eingeladen sind) nach dem derzeitigen Planungsstand am 16. Januar 2016 in Berlin, am 23. April 2016 voraussichtlich in Bielefeld und im Sommer 2016 an einem noch zu bestimmenden Ort. Bitte denken Sie auch an die ULD-Sommerakademie am 19. September 2016 in Kiel und die Vorstandssitzung/Mitgliederversammlung der DVD am 22./23. Oktober 2016 in Bonn. Der neue Vorstand freut sich auf seine Arbeit und steht seinen Mitgliedern für Anregungen und Mitwirkung selbstverständlich gerne zur Verfügung. Sie erreichen uns in unserer neuen Geschäftsstelle in der Reuterstraße 157, 53113 Bonn, unter den unverändert gebliebenen Kontaktdaten (Tel.: 0228/222498, Fax: 0228/2438470; dvd@datenschutzverein.de; www.datenschutzverein.de); wir freuen uns auf Ihre Mitwirkung.

Für den Vorstand – Sönke Hilbrans

Dr. Udo Kauß

Das In-Camera-Verfahren bei den Verwaltungsgerichten

zur Geschichte und zu seiner aktuellen Praxis, zugleich Besprechung des Beschlusses des BVerwG vom 27.10.2014 (20 F 6.14)

I. Die Einführung des In-Camera-Verfahren: ein erster Schritt

Bis 1999 gab es keine gerichtliche Kontrolle der Geheimdienste zu Sachverhalten, die nicht etwa via Presse bzw. die nicht schon selbst von den Geheimdiensten bekannt gemacht worden sind. Kein Beamter des Verfassungsschutzes musste Gerichten Frage und Antwort stehen, wenn der Innenminister dies nicht durch Erteilung einer Ausnahmegenehmigung erlaubt hatte. Wurde diese versagt, dann war hier der Rechtsstaat zu Ende. Dies galt auch, wenn Verwaltungsgerichte das bei Klageverfahren sonst selbstverständliche Recht der Vorlage der Verwaltungsakten bei den Geheimdiensten einforderten. Die Geheimdienste konnten dies verweigern, gestützt auf eine sog. Sperrerklärung des zuständigen Innenministers. Und damit war die gerichtliche Kontrolle zu Ende. Die Dienste brauchten sich von keinem Gericht in die Karten schauen lassen.

Das war die Situation bis 1999. In diesem Jahr befand das Bundesverfassungsgericht (BVerfG) den generellen Ausschluss jeglicher gerichtlicher Kontrolle der Geheimdienste für unvereinbar mit dem verfassungsmäßig verbürgten Recht auf gerichtliche Kontrolle (Justizgewährleistungsrecht in Art. 19 Abs. 4 Grundgesetz – Beschluss v. 27.10.1999, 1 BvR 385/99). Dem folgte der Gesetzgeber im Jahre 2001 mit der Einführung von besonderen Fachsenaten bei den obersten Verwaltungsgerichten (Oberverwaltungsgerichte, in manchen Bundesländern auch Verwaltungsgerichtshöfe genannt, und dem Bundesverwaltungsgericht). Seither müssen auch die Geheimdienste die vollständigen Akten eines konkreten Falles diesen neu gebildeten Fachsenaten vorlegen, wenn ein Verwaltungsgericht sich sonst nicht in der Lage sieht, über die Rechtmäßigkeit des geheimdienstlichen Handelns zu befinden (§ 99 Abs. 2 VwGO).

Die Fachsenate überprüfen nun – in camera = in einer eigenen Kammer – in nicht-öffentlicher und geheimer Sitzung unter Ausschluss des klagenden Bürgers, ob die Verweigerung der Aktenvorlage an das Verwaltungsgericht durch die (zahlreichen) gesetzlichen Ausschlussgründe gerechtfertigt ist. Ausschlussgründe sind, dass die verweigerten Akten bzw. Aktenteile „ihrem Wesen nach“ geheim seien, sie dem „Quellenschutz“ unterliegen, weil z. B. den Spitzeln Vertraulichkeit zugesichert worden ist, weil das „Wohl des Bundes oder eines Landes“ tangiert sei, oder weil generell der „Schutz der Arbeitsweise“ geltend gemacht wird.

Das Wesentliche und Neue ist: Diese Fachsenate können als einziges Gericht und überhaupt einzige Institution außerhalb der Dienste die Vorlage der bisher zurückgehaltenen Aktenteile an die in der Sache befassten Verwaltungsgerichte anordnen, wenn sie, nun in Kenntnis der Akten, nicht den Geheimhaltungsszenarien der Dienste folgen. Und die Dienste müssen ab sofort damit leben, dass es nun immerhin eine gerichtliche Instanz gibt, die die Akten eines konkreten Streitfalles vollständig in Augenschein nehmen darf. Damit hatte Deutschland endlich den Standard erreicht, wie er insbesondere in den USA und skandinavischen Ländern längst erreicht war.

II. Bisherige Erfahrungen

Die Erfahrungen nach 15 Jahren neuer Rechtslage sind durchweg ernüchternd. Dem Autor ist kein Fall bekannt, in dem die Fachsenate wirklich essentielle neue Fakten haben bekannt werden lassen. Als jüngstes Beispiel kann der Beschluss des Verwaltungsgerichtshofes für Baden-Württemberg vom 26.03.2015 (Az: 14 S 310/15) genommen werden. Dort hat die Einschaltung des Fachsenats dazu geführt, dass aus den zu prüfenden 700 qua ministerielle Sperrerklärung umfänglichst geschwärzten Aktenseiten so „geheime“ Informationen wie die Namen zweier früherer Justizminister des Landes wieder entschwärzt und damit offenbart werden sollen. Betroffener Bürger war in diesem Fall ein Freiburger Rechtsanwalt und langjähriges Gemeinderatsmitglied, der über 40 Jahre vom Verfassungsschutz beobachtet worden war (vgl. DANA 4/2014, S. 172). Beim In-Camera-Verfahren des ebenfalls 38 Jahre geheimdienstlich beobachteten Geheimdienstkritikers und Rechtsanwalts Rolf Gössner war der Fachsenat des Bundesverwaltungsgerichts im Jahre 2009 noch vollständig der Schwärzungsorgie des Verfassungsschutzes gefolgt. Von immerhin rd. 2000 zu 90 % geschwärzten Seiten der über Gössner angelegten Verfassungsschutzakte wurde nicht ein Komma als offenbarungsfähig befunden. Die Entscheidung des Bundesverwaltungsgerichts (BVerwG) vom 27.10.2014 deutet nun einen hoffentlich nicht nur kosmetischen Gesinnungswandel an. Sie belegt einen Abgrund von Geheimnistuerei des Verfassungsschutzes, zu deren Verdeckung das Bundesverwaltungsgericht sich nicht hat hergeben lassen.

III. BVerwG: Verfassungsschutz täuscht Verwaltungsgericht!

Durch das 2001 bei den Verwaltungsgerichten eingeführte In-Came-

ra-Verfahren ist die Offenbarung eines unverfrorenen Falles einer Datenverschleierung gelungen: In einem Verfahren auf Auskunft der beim Bundesamt für Verfassungsschutz über den Kläger gespeicherten Daten hat das beklagte Bundesamt für Verfassungsschutz mit ausdrücklicher Zustimmung des Bundesministers des Inneren (BMI) dem Verwaltungsgericht Köln einen geschwärzten NADIS-Ausdruck über den Kläger vorgelegt. Dieser NADIS-Ausdruck war gemäß der Sperrerklärung des BMI genau an der Stelle geschwärzt, wo sonst die Hinweise auf sonstige aktenführende Sicherheitsbehörden angebracht sind. Die Existenz solcher Hinweise hatte der Kläger vermutet, der als Computerfachmann über 10 Jahre im sicherheitsgeprüften Bereich gearbeitet hatte. Weil er die Richtigkeit der zuvor vom Verfassungsschutz im Jahre 2011 erteilten schriftlichen Auskunft bezweifelte und vermutete, dass über die Hinweis-Daten zu seinen zwei Sicherheitsüberprüfungen hinaus keine weiteren Daten zu seiner Person im „Nachrichtendienstlichen Informationssystem“ (NADIS) gespeichert seien, klagte er auf vollständige Auskunft über die zu seiner Person vom Verfassungsschutz gespeicherten Daten. Im Prozess hat das Verwaltungsgericht Köln dem Verfassungsschutz aufgegeben, den angeblich einzig noch existierenden NADIS-Ausdruck zur Person des Klägers vorzulegen. Dem hat sich das Bundesamt zunächst vollständig verweigert. Als das Gericht nicht locker gelassen hat, hat das Bundesamt einen geschwärzten Ausdruck zusammen mit einer Sperrerklärung des BMI vorgelegt. Begründung des BMI: das Bekanntwerden der geschwärzten Informationen würde dem Wohl des Bundes oder eines Landes Nachteile bereiten bzw. die Vorgänge müssten nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden (§ 99 Abs. 1 VwGO).

Das BVerwG hat das Geheimnis der Schwärzungen gelüftet und zu aller Erstaunen festgestellt, dass dort gar nichts zu verdecken war. Offensichtlich sollte dem Verwaltungsgericht und sodann dem Betroffenen gegenüber die Tatsache weiterer Speicherungen bei anderen Sicherheitsbehörden suggeriert werden, obwohl das Amt gar nichts über den Kläger gespeichert hatte und auch keine Hinweise auf Speicherungen ausländischen Sicherheitsbehörden vorhanden waren, wie dies der Kläger vermutet hatte. Das Bundesverwaltungsgericht hat dieses auf Verunsicherung des Klägers angelegten Täuschungsmanöver des Verfassungsschutzes und Ministeriums nicht mitgemacht und die Sperrerklärung des Bundesinnenministeriums für rechtswidrig erklärt und die Vorlage des ungeschwärzten NADIS-Ausdruckes angeordnet.

IV. Erfreuliche Klarstellungen

Das BVerwG hat dem Verfassungsschutz und seinem vorgesetztem Bundesminister des Inneren (BMI) ins Stammbuch geschrieben, dass die Tatsache der Einstufung eines NADIS-Ausdrucks als Verschlusssache-NfD (steht für „nur für den Dienstgebrauch“, Red.) ohne Bedeutung ist. „Denn Unterlagen sind nicht schon deswegen ihrem Wesen nach oder nach einem Gesetz geheim zu halten. Vielmehr kommt es darauf an, ob sich nach den materiellen Maßstäben des § 99 Abs. 1 Satz 2 VwGO eine Geheimhaltungsbedürftigkeit ergibt, ob also der Grund für die Einstufung als Verschlusssache noch fortbesteht…“

Weiter hat sich das BVerwG mit dem Argument des BMI auseinandergesetzt, aus der Schwärzung folge nicht, dass der Auszug – über die zwei offen gelegten Aktenzeichen der Sicherheitsüberprüfungsakten hinaus – weitere Aktenzeichen enthalte. Die Schwärzung sei, so das BMI, vielmehr unabhängig davon erforderlich. Denn andernfalls wäre ein „Umkehrschluss“ möglich, ob aus operativer Sicht empfindliche Informationen zum Kläger über die Sicherheitsüberprüfungsakten hinaus vorlägen. Diese Denke hat das BVerwG klar zurückgewiesen. Zitat: „Mit dieser Begründung lässt sich die Schwärzung des NADIS-Ausdrucks nicht rechtfertigen. Es ist nicht zu erkennen, dass eine vollständige Offenlegung die geheimdienstliche Arbeit erschweren könnte. Der Senat hat den NADIS-Ausdruck im Original in Augenschein genommen und festgestellt, dass die Schwärzung, die sich unterhalb der zwei offen gelegten Aktenzeichen befindet, keine geheimhaltungsbedürftigen Informationen betrifft, sondern lediglich an dieser Stelle ein leeres Blatt verdeckt… Der Beigeladene (das BMI, Red.) bleibt eine Erklärung dafür schuldig, warum der Umstand, dass im NADIS-Ausdruck keine über die erfolgte Offenlegung hinausgehenden Erkenntnisse zur Person des Klägers dokumentiert sind, Rückschlüsse auf ‚aus operativer Sicht empfindliche Informationen‘ erlaubt. Bei einer Offenlegung erfährt der Kläger lediglich, dass im NADIS-Ausdruck keine weiteren Verfahren aufgeführt sind. Ein darüber hinausgehender Erkenntnisgewinn ist damit nicht verbunden. Die Hinweise des Beigeladenen auf den Gesichtspunkt der ‚Spionageabwehr‘ oder der ‚Verstrickung‘ gehen am Fall vorbei. Es erscheint deshalb nicht verständlich, warum die Freigabe dieser ‚Passage‘ gleichwohl die befürchteten Rückschlüsse auf die Informationszugänge der Verfassungsschutzbehörden zulassen soll“.

V. Einziger Zweck: Angst und Unsicherheit

Die Entscheidung des BVerwG offenbart, wie die Geheimdienste und ihre vorgesetzten Aufsichtsbehörden ihre Geheimhaltungsinteressen auch heute noch verstehen. Jeder Schritt zu mehr Transparenz muss mühevollst erkämpft werden. Gesetzliche Vorschriften – das gesetzliche Auskunftsrecht des Bürgers auch gegenüber den Sicherheitsbehörden und das gerichtliche In-Camera-Verfahren – werden durch die Geheimdienste, hier das Bundesamt für Verfassungsschutz, konterkariert, wo dies nur möglich ist. Und sei es nur zu dem einzigen in diesem Fall ersichtlichen Zweck: bei dem betroffenen Bürger Angst und Unsicherheit zu erzeugen.

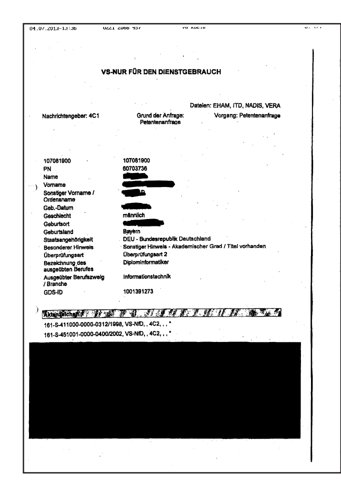
VI. Skandal im Skandal

Das Bundesamt für Verfassungsschutz und der Bundesinnenminister hatten sich darauf 10 Monate geweigert, der Anordnung des Bundesverwaltungsgerichts nachzukommen und den ungeschwärzten NADIS-Ausdruck vom 13.03.2013 dem Verwaltungsgericht vorzulegen. Im August 2015 wurde schließlich, nach mehrfacher dringli-

cher Aufforderung des Verwaltungsgerichts (VG), diesem ein ungeschwärzter NADIS-Ausdruck vorgelegt. Und nun nimmt eine weitere Ungeheuerlichkeit ihren Lauf: Durch Vergleich der sichtbaren Teile des geschwärzten NADIS-Ausdrucks vom 13.03.2013 mit dem dem BVerwG vorgelegten NADIS-Ausdruck vom 04.02.2014 mussten erhebliche Abweichungen von Schriftbild und Reihenfolge der aufgeführten Daten festgestellt werden. Diese führten zu dem begründeten Verdacht, dass das Bundesamt dem BVerwG einen anderen über ein Jahr später gefertigten NADIS-Ausdruck über den Kläger vorgelegt hat. Das Bundesamt für Verfassungsschutz hat in der mündlichen Verhandlung vor dem VG Köln am 01.10.2015 zu Protokoll eingeräumt und zugestanden, dass dem BVerwG im angestrengten In-Camera-Verfahren ein unrichtiger NADIS-Ausdruck vorgelegt worden war. Das wäre aber aus Versehen geschehen durch eine übereifrige Fachabteilung, die ohne Beteiligung des Justiziariats des Bundesamtes einen Ausdruck gefertigt und dem Bundesverwaltungsgericht übermittelt habe. Damit steht fest: Der Verfassungsschutz hat dem Bundesverwaltungsgericht nicht den ursprünglichen (und geschwärzten) NADIS-Ausdruck vom 13.03.2013 vorgelegt. Vielmehr hat der Verfassungsschutz dem Bundesverwaltungsgericht einen ein Jahr später hergestellten Ausdruck vom 04.02.2014 vorgelegt und diesen neu hergestellten NADIS-Ausdruck für die Vorlage beim BVerwG eigens wiederum eingeschwärzt. Wie hatte noch das BVerwG zu diesem wiederum geschwärzten NADIS-Ausdruck ausgeführt (Rn. 9):

„Der Senat hat den NADIS-Ausdruck im Original in Augenschein genommen und festgestellt, dass die Schwärzung, die sich unterhalb der zwei offen gelegten Aktenzeichen befindet, keine geheimhaltungsbedürftigen Informationen betrifft, sondern lediglich an dieser Stelle ein leeres Blatt verdeckt.“

Durch seine Trickserei hat der Verfassungsschutz nicht nur den Kläger und das VG Köln an der Nase herumgeführt, sondern auch noch das Bundesverwaltungsgericht, das seine Entscheidung auf der Grundlage eines falschen NADIS-Ausdruck gefällt hat. Damit hat der Verfassungsschutz verhindert, dass jemals die Wahrheit über den geschwärzten Inhalt im NADIS-Ausdruck vom 13.03.2013 ans Tageslicht kommt. Kommentar des Vorsitzenden Richters beim VG Köln: Bei den Geheimdiensten sei das eben so. Auch Gerichte würden bei Geheimdiensten nicht wirklich hinter die Kulissen schauen können. Damit müsse sich auch der Kläger abfinden. Das alles ist ein erneuter Beweis dafür, dass Geheimdienste weder gerichtlich (noch parlamentarisch) kontrollierbar und daher demokratie-inkompatibel sind (Der vollständige Beschluss des BVerwG ist abrufbar unter http://www.bverwg.de/entscheidungen/entscheidung.php?ent=271014B20F6.14.0).


04.07.2013-13:36 0221 2066 457

VS-NUR FÜR DEN DIENSTGEBRAUCH

Dateien: EHAM, ITD, NADIS, VERA

Nachrichtengeber: 4C1 | Grund der Anfrage: Petentenanfrage | Vorgang: Petentenanfrage

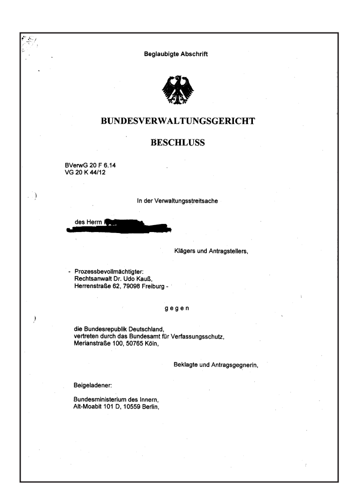
107081900	107081900
PN	60703736
Name	[redacted]
Vorname	[redacted]
Sonstiger Vorname / Ordensname	[redacted]
Geb.-Datum	[redacted]
Geschlecht	männlich
Geburtsort	[redacted]
Geburtsland	Bayern
Staatsangehörigkeit	DEU - Bundesrepublik Deutschland
Besonderer Hinweis	Sonstiger Hinweis - Akademischer Grad / Titel vorhanden
Überprüfungsart	Überprüfungsart 2
Bezeichnung des ausgeübten Berufes	Diplominformatiker
Ausgeübter Berufszweig / Branche	Informationstechnik
GDS-ID	1001391273

Aktenzeichen

161-S-411000-0000-0312/1998, VS-NfD, , 4C2, , , *

161-S-451001-0000-0400/2002, VS-NfD, , 4C2, , , *

[redacted]


Beglaubigte Abschrift

BUNDESVERWALTUNGSGERICHT

BESCHLUSS

BVerwG 20 F 6.14
VG 20 K 44/12

In der Verwaltungsstreitsache

des Herrn [redacted]

Klägers und Antragstellers,

- Prozessbevollmächtigter:
Rechtsanwalt Dr. Udo Kauß,
Herrenstraße 62, 79098 Freiburg -

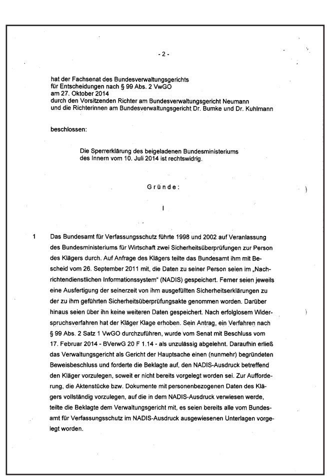
gegen

die Bundesrepublik Deutschland,
vertreten durch das Bundesamt für Verfassungsschutz,
Merianstraße 100, 50765 Köln,

Beklagte und Antragsgegnerin,

Beigeladener:

Bundesministerium des Innern,
Alt-Moabit 101 D, 10559 Berlin,


- 2 -

hat der Fachsenat des Bundesverwaltungsgerichts
für Entscheidungen nach § 99 Abs. 2 VwGO
am 27. Oktober 2014
durch den Vorsitzenden Richter am Bundesverwaltungsgericht Neumann
und die Richterinnen am Bundesverwaltungsgericht Dr. Bumke und Dr. Kuhlmann

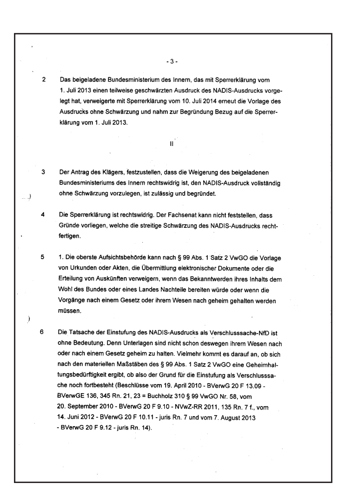
beschlossen:

Die Sperrerklärung des beigeladenen Bundesministeriums des Innern vom 10. Juli 2014 ist rechtswidrig.

Gründe:

I

1 Das Bundesamt für Verfassungsschutz führte 1998 und 2002 auf Veranlassung des Bundesministeriums für Wirtschaft zwei Sicherheitsüberprüfungen zur Person des Klägers durch. Auf Anfrage des Klägers teilte das Bundesamt ihm mit Bescheid vom 26. September 2011 mit, die Daten zu seiner Person seien im „Nachrichtendienstlichen Informationssystem“ (NADIS) gespeichert. Ferner seien jeweils eine Ausfertigung der seinerzeit von ihm ausgefüllten Sicherheitserklärungen zu der zu ihm geführten Sicherheitsüberprüfungsakte genommen worden. Darüber hinaus seien über ihn keine weiteren Daten gespeichert. Nach erfolglosem Widerspruchsverfahren hat der Kläger Klage erhoben. Sein Antrag, ein Verfahren nach § 99 Abs. 2 Satz 1 VwGO durchzuführen, wurde vom Senat mit Beschluss vom 17. Februar 2014 - BVerwG 20 F 1.14 - als unzulässig abgelehnt. Daraufhin erließ das Verwaltungsgericht als Gericht der Hauptsache einen (nunmehr) begründeten Beweisbeschluss und forderte die Beklagte auf, den NADIS-Ausdruck betreffend den Kläger vorzulegen, soweit er nicht bereits vorgelegt worden sei. Zur Aufforderung, die Aktenstücke bzw. Dokumente mit personenbezogenen Daten des Klägers vollständig vorzulegen, auf die in dem NADIS-Ausdruck verwiesen werde, teilte die Beklagte dem Verwaltungsgericht mit, es seien bereits alle vom Bundesamt für Verfassungsschutz im NADIS-Ausdruck ausgewiesenen Unterlagen vorgelegt worden.


- 3 -

2 Das beigeladene Bundesministerium des Innern, das mit Sperrerklärung vom 1. Juli 2013 einen teilweise geschwärzten Ausdruck des NADIS-Ausdrucks vorgelegt hat, verweigerte mit Sperrerklärung vom 10. Juli 2014 erneut die Vorlage des Ausdrucks ohne Schwärzung und nahm zur Begründung Bezug auf die Sperrerklärung vom 1. Juli 2013.

II

3 Der Antrag des Klägers, festzustellen, dass die Weigerung des beigeladenen Bundesministeriums des Innern rechtswidrig ist, den NADIS-Ausdruck vollständig ohne Schwärzung vorzulegen, ist zulässig und begründet.

4 Die Sperrerklärung ist rechtswidrig. Der Fachsenat kann nicht feststellen, dass Gründe vorliegen, welche die streitige Schwärzung des NADIS-Ausdrucks rechtfertigen.

5 1. Die oberste Aufsichtsbehörde kann nach § 99 Abs. 1 Satz 2 VwGO die Vorlage von Urkunden oder Akten, die Übermittlung elektronischer Dokumente oder die Erteilung von Auskünften verweigern, wenn das Bekanntwerden ihres Inhalts dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen.

6 Die Tatsache der Einstufung des NADIS-Ausdrucks als Verschlusssache-NfD ist ohne Bedeutung. Denn Unterlagen sind nicht schon deswegen ihrem Wesen nach oder nach einem Gesetz geheim zu halten. Vielmehr kommt es darauf an, ob sich nach den materiellen Maßstäben des § 99 Abs. 1 Satz 2 VwGO eine Geheimhaltungsbedürftigkeit ergibt, ob also der Grund für die Einstufung als Verschlusssache noch fortbesteht (Beschlüsse vom 19. April 2010 - BVerwG 20 F 13.09 - BVerwGE 136, 345 Rn. 21, 23 = Buchholz 310 § 99 VwGO Nr. 58, vom 20. September 2010 - BVerwG 20 F 9.10 - NVwZ-RR 2011, 135 Rn. 7 f., vom 14. Juni 2012 - BVerwG 20 F 10.11 - juris Rn. 7 und vom 7. August 2013 - BVerwG 20 F 9.12 - juris Rn. 14).

- 4 -

7 Ein Nachteil für das Wohl des Bundes oder eines Landes im Sinne von § 99 Abs. 1 Satz 2 VwGO ist unter anderem dann gegeben, wenn und soweit die Bekanntgabe des Akteninhalts die künftige Erfüllung der Aufgaben der Sicherheitsbehörden einschließlich deren Zusammenarbeit mit anderen Behörden erschweren würde. Die künftige Erfüllung der Aufgaben der Sicherheitsbehörden kann erschwert werden, wenn sich aus einer vollständigen Offenlegung von Unterlagen vor allem im Rahmen einer umfangreichen Zusammenschau Rückschlüsse auf die gegenwärtige Organisation der Sicherheitsbehörden, die Art und Weise ihrer Informationsbeschaffung, aktuelle Ermittlungsmethoden oder die praktizierten Methoden ihrer Zusammenarbeit mit anderen Stellen ableiten lassen (Beschluss vom 4. März 2010 - BVerwG 20 F 3.09 - juris Rn. 6). Zu solchen Rückschlüssen grundsätzlich geeignet sind beispielsweise Vorgangsvorblätter, Aktenzeichen, Organisationskennzeichen und Arbeitstitel, Verfügungen und namentliche Hinweise auf Bearbeiter, Aktenvermerke, Arbeitshinweise, Randbemerkungen und Querverweise sowie Hervorhebungen und Unterstreichungen.

8 Das beigeladene Bundesministerium des Innern trägt vor, aus der Schwärzung folge nicht, dass der Auszug - über die zwei offen gelegten Aktenzeichen der Sicherheitsüberprüfungsakten hinaus - weitere Aktenzeichen enthalte. Die Schwärzung sei vielmehr unabhängig davon erforderlich. Denn andernfalls wäre ein „Umkehrschluss“ möglich, ob aus operativer Sicht empfindliche Informationen zum Kläger über die Sicherheitsüberprüfungsakten hinaus vorlägen.

9 Mit dieser Begründung lässt sich die Schwärzung des NADIS-Ausdrucks nicht rechtfertigen. Es ist nicht zu erkennen, dass eine vollständige Offenlegung die geheimdienstliche Arbeit erschweren könnte. Der Senat hat den NADIS-Ausdruck im Original in Augenschein genommen und festgestellt, dass die Schwärzung, die sich unterhalb der zwei offen gelegten Aktenzeichen befindet, keine geheimhaltungsbedürftigen Informationen betrifft, sondern lediglich an dieser Stelle ein leeres Blatt verdeckt.

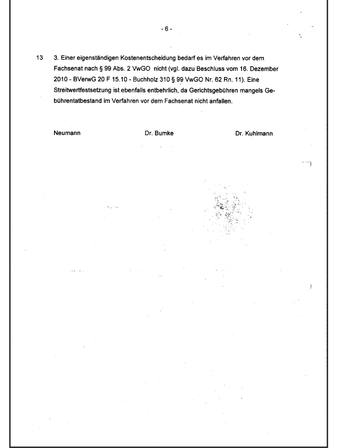
10 Geschwärzt werden dürfen zwar auch Teile eines Dokuments, die für sich genommen nicht geheimhaltungsbedürftig sind, die aber aus dem konkreten Zusammenhang heraus Rückschlüsse auf geheimhaltungsbedürftige Informationen

- 5 -

erlauben. So ist es nicht zu beanstanden, wenn sich - in Einzelfällen - Schwärzungen etwa von Unterstreichungen oder Randzeichen nicht auf eine Unkenntlichmachung an der konkreten Stelle beschränken, sondern auch darüber hinausgreifen, weil andernfalls Rückschlüsse im Hinblick auf das konkrete Erkenntnisinteresse sowie die Arbeitsmethode einer nachrichtendienstlichen Behörde möglich wären (Beschluss vom 1. Februar 2011 - BVerwG 20 F 17.10 - juris Rn. 5). Entscheidend ist, ob mit einer Offenlegung ein Erkenntnisgewinn in Bezug auf den berechtigten Geheimhaltungsgrund verbunden ist (vgl. auch Beschluss vom 1. August 2011 - BVerwG 20 F 26.10 - juris Rn. 10). Danach können auch Schwärzungen von Leerstellen in einem Dokument gerechtfertigt sein. Zur Begründung genügt es aber nicht, pauschal auf einen möglichen „Umkehrschluss“ zu verweisen.

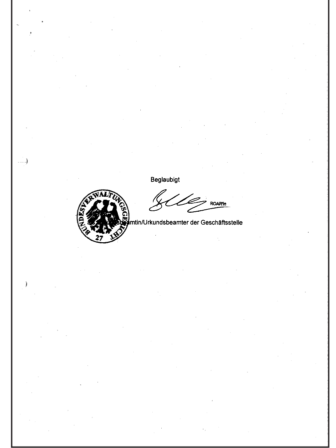
11 Der Beigeladene bleibt eine Erklärung dafür schuldig, warum der Umstand, dass im NADIS-Ausdruck keine über die erfolgte Offenlegung hinausgehenden Erkenntnisse zur Person des Klägers dokumentiert sind, Rückschlüsse auf „aus operativer Sicht empfindliche Informationen“ erlaubt. Bei einer Offenlegung erfährt der Kläger lediglich, dass im NADIS-Ausdruck keine weiteren Verfahren aufgeführt sind. Ein darüber hinausgehender Erkenntnisgewinn ist damit nicht verbunden. Die Hinweise des Beigeladenen auf den Gesichtspunkt der „Spionageabwehr“ oder der „Verstrickung“ gehen am Fall vorbei. Es erscheint deshalb nicht verständlich, warum die Freigabe dieser „Passage“ gleichwohl die befürchteten Rückschlüsse auf die Informationszugänge der Verfassungsschutzbehörden zulassen soll.

12 2. Darüber hinaus sind auch die Ermessenserwägungen nicht tragfähig. Der Beigeladene verkennt die Eigenständigkeit der im Rahmen des § 99 Abs. 1 Satz 2 VwGO geforderten Ermessensausübung. In der Sperrerklärung wird zwar der Maßstab für die Ermessensausübung zutreffend wiedergegeben (vgl. dazu nur Beschluss vom 21. Februar 2008 - BVerwG 20 F 2.07 - BVerwGE 130, 236 - juris Rn. 18). Der Beigeladene beschränkt sich dann aber darauf, lediglich die bereits angeführten Gründe für die behauptete Geheimhaltungsbedürftigkeit zu wiederholen. Damit verstellt er sich den Blick dafür, dass der Fall - entgegen seiner Annahme - angesichts des Zeitablaufs Besonderheiten aufweist, die im Rahmen der Ermessensausübung zu berücksichtigen gewesen wären.


- 6 -

13 3. Einer eigenständigen Kostenentscheidung bedarf es im Verfahren vor dem Fachsenat nach § 99 Abs. 2 VwGO nicht (vgl. dazu Beschluss vom 16. Dezember 2010 - BVerwG 20 F 15.10 - Buchholz 310 § 99 VwGO Nr. 62 Rn. 11). Eine Streitwertfestsetzung ist ebenfalls entbehrlich, da Gerichtsgebühren mangels Gebührentatbestand im Verfahren vor dem Fachsenat nicht anfallen.

Neumann | Dr. Bumke | Dr. Kuhlmann


Beglaubigt

ROAR'in

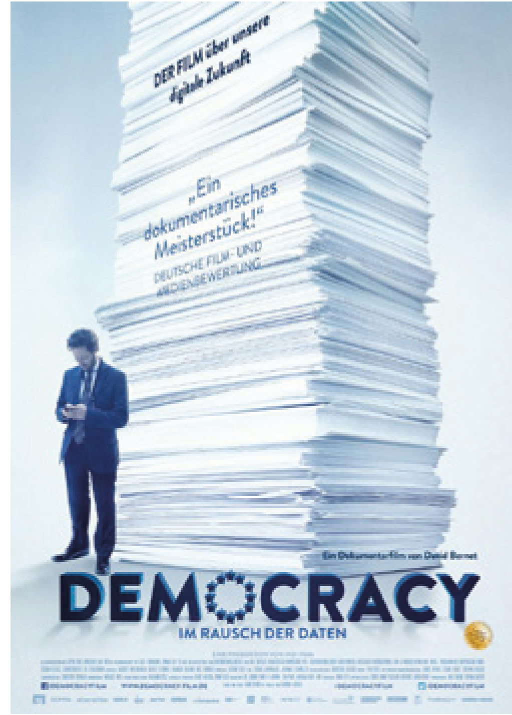
...mtin/Urkundsbeamter der Geschäftsstelle

Werner Hülsmann

Democracy – Im Rausch der Daten

Nicht nur eine Filmbesprechung

Die Berlin-Premiere dieses Films, der seit dem 12. November in einigen Kinos läuft, fand im Beisein des Regisseurs David Bernet und der Protagonisten Viviane Reding (Vizepräsidentin der Europäischen Kommission a.D., Mitglied des Europäischen Parlaments) und Jan Philipp Albrecht (Europaabgeordneter der Grünen, EU-Berichterstatter) samt seinem Mitarbeiter Ralf Bendrath sowie Dr. Alexander Dix, Berliner Beauftragter für Datenschutz und Informationsfreiheit, am 6. November 2015 in der gut besuchten Urania statt.



Die Farbfilm Verleih GmbH, schreibt über den – in schwarz/weiß gehaltenen Film – zutreffend: „Mit DEMOCRACY – IM RAUSCH DER DATEN eröffnet uns Regisseur David Bernet einen erstaunlichen Einblick in den Gesetzgebungsprozess auf EU-Ebene. Eine fesselnde und hochbrisante Geschichte über eine Handvoll Politiker, die versucht, die Gesellschaft in der digitalen Welt vor den Gefahren von Big Data und Massenüberwachung zu schützen.“ Jan Philipp Albrecht hat als Berichterstatter des LIBE-Ausschusses die – zeitweise kaum realisierbar wirkende – Aufgabe, nicht nur die fast 4.000 Änderungsanträge in den Kommissionsentwurf einzuarbeiten, sondern zusammen mit den sogenannten Schattenberichterstattern der anderen Fraktionen einen Kompromiss zu finden, der erst im Ausschuss und dann auch im Parlament eine große Mehrheit finden kann. Vertreterinnen und Vertreter unterschiedlicher Lobbygruppen kommen in dem Film ebenso zu Wort, wie Sprecherinnen und Sprecher von Datenschutzorganisationen, deren unterschiedliche Interessen gut dargestellt werden.



Auch wenn den meisten Zuschauerinnen und Zuschauern bereits bekannt gewesen sein dürfte, wie das Ergebnis dieser Arbeit – nämlich die vom EU-Parlament vorgeschlagene Fassung des Verordnungsentwurfs – aussieht, ist der Film spannend und aufschlussreich. Das Endergebnis des Gesetzgebungsprozesses – also die vom Rat und vom EU-Parlament verabschiedete EU-Datenschutzgrundverordnung – lag zum Zeitpunkt des Redaktionsschlusses noch nicht vor. Auch dies ist exemplarisch für den europäischen Gesetzgebungsprozess. In keinem demokratischen Staat muss noch ein Ministerrat über ein vom Parlament beschlossenes Gesetz entscheiden, damit es veröffentlicht und in Kraft treten kann.

In dem anschließendem von Dr. Wolf Siegert moderierten Publikumsgespräch wurde unter anderem deutlich, dass die Verhandlungen im Ministerrat und leider auch die Trilog-Verhandlungen an der für ein demokratisches Gemeinwesen erforderliche Transparenz vermissen lassen. Auf die eher scherzhafte Nachfrage an den Regisseur, ob er jetzt einen Teil 2 über die Trilog-Verhandlungen drehen würde, antwortete dieser: Er könne sich nicht vorstellen, dass dies möglich sei. Während die Abgeordneten des Europaparlaments sehr unbefangen mit den Kameras umgingen, sei es doch schwierig gewesen, bei Ministerratssitzungen zu filmen. Reding und Albrecht betonten, dass die Aussagen der Minister vor ihren nationalen Parlamenten und in ihren „Sonntagsreden“ wenig mit dem zu tun hätten, was sie im Rat äußern und fordern.

Fazit: Der Film ist – unabhängig davon, wie die Trilogverhandlungen ausgehen werden – unbedingt sehenswert und stellt am Beispiel der Europäischen Datenschutzgrundverordnung sehr gut dar, wie Politik in der EU gemacht wird. Die unterschiedlichen Interessen der verschiedenen Akteure und Lobbygruppen zum Datenschutz werden ebenfalls gut deutlich. Daher ist dieser Film „ein Muss“ für alle, die an Datenschutzpolitik und den Europäischen Gesetzgebungsprozessen interessiert sind. Dies gilt umso mehr, wenn – wie bei vielen Vorführungen in Programmkinos – anschließend eine Publikumsdiskussion stattfindet.

Weitere Informationen finden sich auf http://www.democracy-film.de/

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Merkel gegen zu viel Datenschutz

Bundeskanzlerin Angela Merkel hat die deutsche Bevölkerung aufgefordert, endlich ihre ständigen Datenschutz-Bedenken fallen zu lassen und den Schutz ihrer Privatsphäre der Weiterentwicklung der nationalen Wirtschaft unterzuordnen. Nur so könne man im digitalen Zeitalter international mithalten. Die umfassende Sammlung und Auswertung von Nutzerdaten ist die Grundlage des Erfolgsrezeptes von US-Firmen wie Google oder Facebook. Deutsche Internet-Firmen beklagen immer wieder, dass die hiesigen Datenschutz-Regelungen sie daran hindern, ähnliche Entwicklungen vollziehen zu können. Laut Merkel müsse daher ein Umdenken stattfinden.

Merkel erklärte auf einem Kongress des CDU-Wirtschaftsrates im Juni 2015 sowie auf einem CDU-Kongress zum digitalen Wandel am 12.09.2015: „Wer Daten als eine Bedrohung wahrnimmt, wer immer nur darüber nachdenkt, welchen Schaden jedes Stück Information anrichten kann, wird nicht in der Lage sein, die Möglichkeiten der Digitalisierung zu seinem Vorteil zu nutzen." Big Data sei keine Bedrohung, sondern „der Rohstoff der Zukunft". Wertschöpfung entstehe künftig nicht mehr hauptsächlich über die maschinelle Herstellung eines Produkts, sondern vor allem über die Nutzung von Kundendaten. „Wenn wir aber die Verbindung zum Kunden dann nicht richtig aufbauen, dann wird uns ein wesentlicher Teil der Wertschöpfung verloren gehen." Dies werde dann „irgendwo in Amerika oder Asien" stattfinden. Der Wettlauf werde in 5 bis 10 Jahren entschieden sein.

Wenn die Möglichkeiten, die hier entstünden, nicht ausgenutzt werden, werde man früher oder später auf große Probleme zusteuern. Merkel merkte an, dass im Zuge einer neuen Automatisierungswelle, die durch neue Entwicklungen in der IT-Forschung ausgelöst wird, zahlreiche Arbeitsplätze verschwinden und durch Maschinen ersetzt werden. „Aber ich bin zuversichtlich, dass viel mehr Arbeitsplätze durch die Wertschöpfung aus Daten geschaffen werden können" (Nicht zu viel Datenschutz, SZ 14.09.2015, Kahle, Merkel: Deutsche sollen Datenschutz für die Wirtschaft aufgeben, winfuture.de, 10.06.2015).

Bund

Regierungskoalition plant verbesserte Geheimdienstkontrolle

Die parlamentarische Kontrolle der Nachrichtendienste soll nach Plänen von Union und SPD durch einen „Ständigen Sachverständigen" mit einem eigenen Apparat verbessert werden. Die für Geheimdienstkontrolle zuständigen FachpolitikerInnen der großen Koalition haben sich hierauf geeinigt und reagieren damit auf wiederholte Geheimdienstaffären sowie die Erkenntnis, dass die bisherige parlamentarische Kontrolle der Dienste unzureichend ist. Über die Eckpunkte der Reform haben sich die zuständigen FachpolitikerInnen der Union, Clemens Binninger (CDU) und Stephan Mayer (CSU) Eva Högl und Burkhard Lischka (SPD) schon vor der Sommerpause 2015 geeinigt.

Abgeordnete hatten immer wieder beklagt, dass ihnen für nachhaltige Kontrolle die Zeit fehlt. Derzeit müssen 13 Personen – 9 Abgeordnete des Parlamentarischen Kontrollgremiums (PKG) und 4 Mitglieder der sog. G-10-Kommission – die Arbeit von mehr als 10.000 deutschen GeheimdienstlerInnen kontrollieren. Es gibt keinen entsprechend ausgestatteten Apparat, der ihnen ausreichend zuarbeiten kann. Die Zustimmung von SPD und Union zu den Vorschlägen gilt als sicher. Das die Aufsicht über die Geheimdienste wahrnehmende Kanzleramt signalisierte keine ernsthaften Bedenken. Ein Gesetzentwurf zur besseren Kontrolle der Nachrichtendienste mit dem Sachverständigen-Modell soll bis Ende 2015 in den Bundestag eingebracht werden.

Der „Ständige Sachverständige", in Koalitionskreisen „Geheimdienstbeauftragter light" genannt, soll nicht nach außen auftreten und keine eigenen öffentlichen Erklärungen abgeben. Seine Aufgabe bestünde in der Unterstützung der zuständigen Expertengruppen des Bundestages wie das Parlamentarische Kontrollgremium, das Vertrauensgremium und die G-10-Kommission. Er soll mit drei bis vier Referaten und 20 bis 30 Mitarbeitenden ausgestattet werden. Bislang gibt es nur ein Ausschusssekretariat und eine „Task Force". Einen eigenständigen Geheimdienstbeauftragten soll es nicht geben, weil dieser in Konkurrenz zu den parlamentarischen Kontrolleuren treten könnte. Anders als bei den bisher eingesetzten Sachverständigen, die zumeist ehemalige Bundesrichter mit begrenztem Auftrag waren, soll der Neue kein Pensionär sein und dem Parlament mindestens für die Dauer einer Legislaturperiode zur Verfügung stehen. Seine Besoldung soll vergleichsweise attraktiv sein. Ermittlungsrichter am Bundesgerichtshof, Bundesanwälte oder erfahrene Oberstaatsanwälte kämen bei einer Stellenausschreibung als Kandidaten infrage (Leyendecker/Mascolo, Mehr Kontrolle über Geheimdienste, Prantl, Ein Notstand wird beseitigt, SZ 26.08.2015, 1, 4).

Bund

BMI plant neue Abhörbehörde

Das Bundesinnenministerium (BMI) will eine neue sog. Sicherheitsbehörde aufbauen, mit deren Hilfe die Internet-

kommunikation besser überwacht und Verschlüsselungen gebrochen werden können. Die neue Behörde soll z. B. in die verschlüsselte Kommunikation von Messengerdiensten eindringen können oder die Instrumente für die Kompromittierung von Rechnern für Zwecke der Online-Durchsuchung liefern. Dafür will das BMI KryptologInnen und NetzwerkexpertInnen einstellen. Die Einrichtung soll nicht selbst überwachen, sondern nur die Technik dafür entwickeln; die Anwendung würde weiterhin den operativen Behörden, etwa dem Bundeskriminalamt oder dem Bundesamt für Verfassungsschutz überlassen. Die regierungsintern umstrittenen Pläne von Minister Thomas de Maizière sollen zunächst den Abgeordneten des Bundestags präsentiert werden (Abhören leichter gemacht, Der Spiegel 46/2015, 26).

Bund

Geodaten-CoC als Verhaltensregel anerkannt

Um Unternehmen eine praktikable und rechtssichere Handhabung der Datenschutzregeln bei der Nutzung personenbezogener Geodaten zu ermöglichen, hat die Kommission für Geoinformationswirtschaft (GIW-Kommission) beim Bundesministerium für Wirtschaft und Energie die Bestimmungen der Datenschutzgesetze des Bundes und der Länder zu einem bundesweit einheitlichen Regelwerk zusammengefasst, dem „GeoBusiness Code of Conduct“ (GeoBusiness-CoC). Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Dr. Alexander Dix, hat den GeoBusiness CoC nach § 38a Bundesdatenschutzgesetz (BDSG) offiziell anerkannt.

Brigitte Zypries, Parlamentarische Staatssekretärin beim Bundesminister für Wirtschaft und Energie, begrüßte, dass mit dem GeoBusiness-CoC nun eine bundesweit datenschutzrechtlich anerkannte Selbstverpflichtungserklärung für den Umgang mit personenbezogenen Geodaten in der Wirtschaft vorliegt. Unternehmen können über das zugehörige Online-Zertifizierungsportal mit wenigen Klicks ihren datenschutzkonformen Umgang mit personenbezogenen Daten gegenüber öffentlichen Stellen und Datenanbietern nachweisen. Das erleichtere gerade für kleine und mittelständische Unternehmen den Bezug und die Nutzung von Geodaten und stärke die Anwendung der Datenschutzgesetze. Die wirtschaftliche Nutzung von Geodaten öffentlicher Stellen berge erhebliches wirtschaftliches Potenzial. Dies gelte insbesondere für hochauflösende und genaue Geodaten. Solche Daten weisen allerdings häufig einen Personenbezug auf und sind somit datenschutzrelevant. Konkret geht es dabei z. B. um Eigentümerinformationen in Grundstücksdaten, die von der Rohstoffwirtschaft genutzt werden können, um ihre Betriebsplanung weiter zu verbessern, oder Angaben zu denkmalgeschützten Gebäuden, die für die Versicherungswirtschaft relevant sind.

Der GeoBusiness-CoC wird von der GIW-Kommission in Kooperation mit dem Verein Selbstregulierung Informationswirtschaft e.V. (SRIW) umgesetzt. SRIW Vorstandschef Harald Lemke erklärte: „Durch die Kooperation zwischen Wirtschaft und Behörden ist es gelungen, eine praktikable Lösung zu entwickeln, die Geodaten besser zugänglich macht und zugleich den Datenschutz sichert. Das hat Vorbildcharakter.“ Der Berliner Beauftragte für Datenschutz und Informationsfreiheit Dr. Alexander Dix sieht in dem GeoBusiness-CoC einen angemessenen „Ausgleich zwischen Datenschutz und Informationsfreiheit gefunden worden, der dem Bundesdatenschutzgesetz entspricht.“

Für die Zertifizierung nach dem CoC kann man den Link www.geodatenschutz.org nutzen. Dort werden bestimmte technische und organisatorische Regelungen des Unternehmens in Bezug auf den Datenschutz abgefragt, zum Beispiel wie ein betrieblicher Datenschutzbeauftragter erreichbar ist oder welche Maßnahmen zum Schutz vor unbefugten Zugriffen auf personenbezogene Daten getroffen werden. Dr. Jörg Reichling, Verhandlungsführer für die GIW-Kommission, erläuterte: „Dieses zu harmonisieren haben wir 2010 begonnen, ohne einheitlich geregelten Datenschutz gibt es keinen wirtschaftlichen Mehrwert“ (Staatssekretärin Zypries begrüßt Anerkennung einheitlicher Datenschutzvorgaben für Geodaten durch Aufsichtsbehörden, www.geobusiness.org 03.08.2015).

Bund

Bundesbank will umfassendes Kreditregister

Bei der Aufsichtsbehörde für das Kreditwesen, der Deutschen Bundesbank in Frankfurt, denkt man darüber nach, sämtliche Daten über Kreditgewährungen durch Banken zu erheben und zentral zu speichern. Jeder Kleinstkredit, egal ob ihn eine Privatperson oder eine juristische Person in Anspruch genommen hat, soll gemäß der Vorstellung der Bundesbank von den kreditgebenden Banken an sie gemeldet werden. Entschieden ist noch nichts, doch der Plan sorgt schon im Vorfeld für Widerspruch. Ziel der Maßnahme ist die Stärkung der Finanzstabilität. Bislang weiß die Bundesbank nicht, dass sich ein Bürger bei vielen Banken mehrere Kredite geben lässt. Wenn sehr viele Privathaushalte und Unternehmen sich dadurch in eine Schuldenfalle manövrieren würden, dann könnte dieser Umstand die Finanzstabilität eines ganzen Landes gefährden, etwa wenn die Kredite ausfallen und die Banken aus diesem Grund ins Wanken geraten.

Die Planung ist eine Reaktion der Aufseher auf die globale Finanzkrise. Als die US-Investmentbank Lehman Brothers 2008 pleiteging, stellte man fest, wie wenig Bankkontrolleure über die Kreditrisiken des Bankensektors wussten. Man hatte diese Gefahren lange unterschätzt. Bundesbank-Vizepräsidentin Claudia Buch erläuterte: „Die Erfahrung aus den USA zeigt, dass eine Lockerung der Kreditvergabestandards an bonitätsschwache Haushalte eine der wesentlichen Ursachen für Finanzkrisen sein kann.“ Eine solche Entwicklung könne nur mit granularen Daten identifiziert werden.

- Die Pläne der EZB

Die auch in Frankfurt residierende Europäische Zentralbank (EZB) hat deshalb im Juni 2014 beschlossen, ein zentrales Kreditregister für Europas Finanzsektor aufzubauen. Es sollen dazu eng-

maschige Kundendaten bei den größten Banken Europas, die von der EZB seit knapp einem Jahr beaufsichtigt werden, erhoben werden. So strebt die EZB eine vergleichbare Datenbasis über alle Großbanken in den 19 Euro-Staaten an. Idealerweise würde im Ernstfall ein Blick genügen, um erkennen zu können, wo sich Überschuldungswellen aufbauen, die das System destabilisieren.

Die EZB hatte ursprünglich eine Meldeschwelle von 50.000 Euro vorgesehen, jetzt sollen es 25.000 Euro sein. Noch im Oktober 2015 wollte die EZB einen ersten Beschluss in dieser Sache fassen, dem dann voraussichtlich eine Umfrage bei den betroffenen Banken folgt. Die Umsetzung soll im zweiten Halbjahr 2017 folgen. Zunächst müssten dann Ausleihungen an Firmenkunden und die öffentliche Hand gemeldet werden, später, ab 2020, dann auch weitere Darlehen wie Wohnungsbaukredite oder Dispokredite an private Haushalte. Eine Meldeschwelle von null Euro, wie ihn die Bundesbank für den deutschen Bankensektor erwägt, ist bei der EZB wohl vom Tisch.

- Widerstand

Die Banken in Deutschland wehren sich vehement gegen die Pläne der Aufsicht ohne jegliche Meldeschwelle. Die Institute fürchten den Aufwand. Sie halten dies zudem für viel zu bürokratisch und datenschutzrechtlich heikel. Die Institute müssten viele Details übermitteln, etwa die Art des Kredits, dessen Laufzeit und Währung. Die Bankenlobby schätzt, dass sich die Zahl der zu meldenden Kreditmerkmale gegenüber heute verdreifachen würde.

In einem Schreiben der Deutschen Kreditwirtschaft, der gemeinsamen Lobbyplattform für Sparkassen, Genossenschaftsbanken und Privatbanken, an die Bundesbank heißt es, wenn künftig z. B. auch Dispo-Kredite gemeldet werden müssten, seien die Banken gezwungen, die Kunden bereits bei der Eröffnung von Girokonten nach Einkommen und Vermögen zu befragen. „Bei Wohnungsbaukrediten wird dies seitens der Kunden naturgemäß akzeptiert, ob dies jedoch bei der Eröffnung eines Girokontos der Fall ist, erachten wir als fraglich.“ Der Bearbeitungsprozess werde auf jeden Fall deutlich bürokratisiert, weil die Kunden unter anderem über die Verwendung der Daten und die Meldung an die Bundesbank aufgeklärt und informiert werden müssten. „Unserer Einschätzung nach rechtfertigt der versprochene Nutzen im Sinne Geldpolitik und Finanzmarktstabilität diesen Ansatz in keinster Weise.“ Bei bestehenden Verbindungen müssten die Attribute nicht nur bei reinen Kreditkunden, sondern bei allen Girokunden, denen ein Dispositionskredit eingeräumt wurde, nacherhoben werden, was zu weiteren erheblichem Aufwand führen würde.

- Erwartungen

Die Bundesbank hält bisher an ihren Planungen fest. Es gibt auch andere Aufsichtsbehörden in der Euro-Zone, die alle Daten zur Kreditvergabe einfordern. Die EZB-Regel ist das eine, auf nationaler Ebene dürfen die Aufseher aber jederzeit noch mehr Daten erheben. Bei der Bundesbank heißt es, man könne sich viele Sonderumfragen bei Banken ersparen, wenn die Datenlage besser wäre. In Bezug auf die Immobilienmärkte fehlen Informationen für eine adäquate Risikoeinschätzung, so Peter Barkow, Gründer der Finanzierungsberatung Barkow Consulting, der seit Jahren den Immobilienmarkt analysiert: „Auch wenn es viele Studien dazu gibt: Es ist nach wie vor sehr schwer, wirklich valide Aussagen über die Preise deutscher Wohnimmobilien zu treffen.“ Es gebe zwar viele Daten und Indizes, aber die Ergebnisse seien zum Teil widersprüchlich. Bei gewerblichen Immobilien, dazu gehörten Büro- oder Logistikimmobilien, sei der Nachholbedarf noch größer. „Für diesen Markt gibt es noch weniger Daten und keinerlei Leitindex. Die Datensammlung der Bundesbank könnte das unter Umständen verbessern.

Die Deutsche Bundesbank würde auch einen Überblick über die Gesamtverschuldung der Einzelhaushalte erhalten. Datenschutzrechtliche Einwände weist man zurück, da die Daten anonymisiert würden, so Bundesbank-Vizepräsidentin Buch: „Mit deren Hilfe lassen sich Einzelkreditdaten und Bankbilanzdaten verknüpfen. Eine solche Datenbasis würde uns gute Analysemöglichkeiten für viele Anwendungen bieten“ (Schreiber/Zydra, Frankfurter Datensammler, SZ 10.09.2015, S. 14).

Bund

BDSW fordert Wachleute-Überprüfung

Der Bundesverband der Sicherheitswirtschaft (BDSW) fordert von den Bundesländern strengere Überprüfungen von privaten Wachmännern, die in Flüchtlingsunterkünften arbeiten. Der Hauptgeschäftsführer des Bundesverbandes der Sicherheitswirtschaft, Harald Olschok, meinte: „Es ist überhaupt nicht hinnehmbar, dass Rechtsextreme für solche Tätigkeiten zum Einsatz kommen.“ Kurz zuvor war bekannt geworden, dass im sächsischen Heidenau ein bekennender Neonazi als Sicherheitsmann in einem Flüchtlingsheim eingesetzt wurde.

Fälle mit Wachmännern aus der rechtsextremen Szene sind auch aus Jena und Brandenburg bekannt geworden. Im September 2014 erfolgte eine Misshandlung eines Flüchtlings durch einen Wachmann in einem Heim in Burbach (Nordrhein-Westfalen).

Deutschlandweit waren im September 2015 rund 5.000 private Sicherheitskräfte in Flüchtlingsunterkünften aktiv, eine Zahl, die sich, gemäß Olschok, innerhalb eines Jahres verdoppelt hat. Angesichts der steigenden Flüchtlingszahlen beauftragen Länder und Kommunen immer häufiger private Sicherheitskräfte zum Schutz der Heime. Auch Wachmänner mit Migrationshintergrund seien zunehmend gefragt, da diese häufig die Muttersprache der Flüchtlinge sprechen und leichter bei religiösen Konflikten zwischen verschiedenen Flüchtlingsgruppen vermitteln können.

Die privaten Sicherheitsunternehmen können bislang nur einmalig eine Überprüfung der Mitarbeitenden über das polizeiliche Führungszeugnis aus dem Bundeszentralregister (BZR) vornehmen. Liegen keine Einträge wegen aktueller Straftaten vor, so werden die Bewerbenden eingestellt. Für alle weitergehenden Informationen - etwa eine Abfrage zu einer möglichen rechtsextremen Gesinnung der Wachleute - ist

der Verfassungsschutz zuständig. Die Bundesländer hätten, so Olschok, die Möglichkeit, gerade für den Einsatz in Flüchtlingsheimen das Personal entsprechend überprüfen zu lassen. Hiervon werde offensichtlich noch zu wenig Gebrauch gemacht. In Sachsen gibt es etwa 12.000 private Wachmänner, wovon 3-4% in Flüchtlingsheimen im Einsatz sind. Olschok meinte, eine rechtsextreme Gesinnung sei bei den privaten Sicherheitskräften „genauso stark verbreitet, wie im Durchschnitt der Bevölkerung auch“: „Wir sind ein Spiegelbild der Gesellschaft.“ Gerade in einer Region, wo die Bereitschaft der Bevölkerung geringer sei, Flüchtlinge aufzunehmen, sollten die Anforderungen an private Sicherheitsdienste und deren Beschäftigte besonders hoch und die Zusammenarbeit mit der Polizei zwingend vorgeschrieben sein. Zudem sollten die Unternehmen die Möglichkeit haben, ihre Mitarbeitenden regelmäßig, z. B. jährlich, über BZR auf Straftaten hin abzufragen (Private Wachleute in Flüchtlingsheimen sollten strenger geprüft werden, www.evangelisch.de 03.09.2015).

Bund

Siegel für Gesundheits-Apps?

In einem Brief der beiden stellvertretenden Vorsitzenden der CDU/CSU-Bundestagsfraktion Gitta Connemann und Georg Nüßlein fordern diese, verbindliche Sicherheitsvorgaben für Gesundheits-Apps einzuführen, mit denen digital z. B. der Fitnesszustand oder das Gewicht kontrolliert werden: “Es fehlen klare Regelungen.” Der Brief fordert die Vergabe eines “Siegels für Apps”, das belegt, dass die Daten “in der Hoheit des Nutzers bleiben und nicht weitergegeben werden.” Jede App solle ein Impressum mit Angaben zum Urheber und zur Aktualität enthalten. Auf EU-Ebene müsse sich die Regierung für verbindliche Standards einsetzen, “um möglicherweise gesundheitsgefährdende Anwendungen zu verhindern”. Das von Bundesgesundheitsminister Hermann Gröhe geplante E-Health-Gesetz enthält keine derartigen Vorgaben für Gesundheits-Apps. Inzwischen soll es 400.000 derartiger Onlineangebote für das Smartphone geben; teilweise werden diese von Krankenkassen oder von der Pharmaindustrie angeboten (Mehr Sicherheit für Gesundheits-Apps, Der Spiegel 38/2015, 12).

Hessen

Joschka Fischers Polizeiakte herrenlos im Flughafen

Zollbeamte haben in einem herrenlosen Koffer am Frankfurter Flughafen die Polizeiakte des ehemaligen Außenministers Joschka Fischer gefunden. Darin soll gemäß Presseberichten die Verstrickung Fischers in die damalige linksradikale Szene dokumentiert sein. So wurde Fischer 1976 bei einer Demonstration für die RAF-Terroristin Ulrike Meinhof festgenommen und erkennungsdienstlich behandelt. Damals wurde gegen Fischer wegen Landfriedensbruchs, versuchten Mordes und der Bildung einer kriminellen Vereinigung ermittelt. Die Akte galt seit 1985 als verschollen (Joschka Fischers Polizeiakte gefunden, Polizeiakte, SZ 12./13.09.2015, 4, 12).

Niedersachsen

VHV mit Pay-as-you-drive-Tarif

Nach versuchsweisen Markteinführungen durch andere Versicherungen bietet die VHV-Versicherung auf breiter Front einen Telematik-Tarif an, bei dem weniger Prämie zu zahlen ist, wer wenig und vorsichtig fährt, sich an die Verkehrsregeln hält und Landstraßen meidet. Im Gegenzug werden die KundInnen umfassend kontrolliert und die Fahrdaten erfasst und ausgewertet. VHV-Vorstandsmitglied Per-Johan Horgby erklärte bei der Vorstellung am 30.09.2015: „Das ist ein Meilenstein; wir sind extrem stolz. In der traditionellen Versicherung fragen wir den Kunden: Wer bis Du? Jetzt fragen wir: Wie fährst Du?“ Generali und die Sparkassendirektversicherung wollen mit ähnlichen Angeboten in Kürze auch auf dem Markt groß einsteigen, jedoch mit einem anderen technischen System. Bei VHV wird eine kleine schwarze Box in die 12-Volt-Buchse des Zigarettenanzünders gesteckt, über den die Daten erfasst werden. Ein Nachlass von bis zu 30% auf die Normalprämie ist möglich, wenn die FahrerIn bei vier Kriterien günstig abschneidet: Einhaltung von Tempolimits, Beschleunigungs- und Bremsverhalten, Straßentyp und Uhrzeit der Fahrten. Nachtfahrten erhöhen die Prämie. Horgby meint, das neue System sei datensparsamer als das bisherige: In herkömmlichen Tarifen würden bis zu 50 Kriterien abgefragt, um das Unfallrisiko einzuschätzen, z. B. ob die KundIn ein Eigenheim besitzt: „Wer zur Miete wohnt, muss mehr zahlen. Ist das gerecht?“ Die Nutzung der Box kostet die KundIn 6,99 € pro Monat. Der Tarif lohnt sich daher nur bei hohen Prämien, etwa bei FahranfängerInnen. Horgby sieht keine Datenschutzprobleme. Alle Informationen stünden allein dem Kunden zur Verfügung. VHV-Mitarbeitende hätten keinen Einblick. Die Daten werden von dem Dienstleister Akquinet in Hamburg aufbereitet und gespeichert (Scheuermann, „Wir fragen: Wie fährst du?“ Kieler Nachrichten 01.10.2015, 5).

Nordrhein-Westfalen

Namensänderung zwecks Verhinderung von Diskriminierung

Der frühere Präsident des Verfassungsgerichts von Nordrhein-Westfalen, Michael Bertrams, hat sich dafür ausgesprochen, AusländerInnen leichter den Wechsel zu einem deutschen Namen zu ermöglichen. Wenn Familien mit ausländischen Wurzeln ihren fremd klingenden Namen ändern wollten, um dadurch mögliche Diskriminierungen insbesondere ihrer Kinder zu verhindern, sollten Verwaltungen und Gerichte dies als einen „wichtigen Grund“ akzeptieren. Einen solch wichtigen Grund verlangt das deutsche Namensrecht bei einem Namenswechsel: „Wer sich gegen eine Diskriminierung erfolgreich zur Wehr gesetzt hat, ist vor Wiederholungen keineswegs sicher, solange er den Namen trägt, an dem sich die Diskriminierung

festmacht.“ Wirklichen Schutz könne nur eine Namensänderung bieten.

Hintergrund ist ein Urteil des Verwaltungsgerichts Braunschweig. Dieses hatte den beantragten Namenswechsel einer türkischen Familie mit deutschem Paß mit der Begründung abgelehnt, ein ausländischer Nachname reiche als Grund für eine Namensänderung allein nicht aus. Vielmehr müssten die Betroffenen auch schwerwiegende Beeinträchtigungen aufgrund ihres Namens nachweisen können. Bertrams sieht dies anders. Gerade Menschen mit türkischen Namen seien im wirtschaftlichen und sozialen Leben in Deutschland nach wie vor mit erheblichen Vorurteilen konfrontiert (Diskriminierende Namen, SZ 29.07.2015, 6).

Schleswig-Holstein

Keine anonymen Bestattungen mehr in St. Georg

Auf dem 700 Jahre alten Friedhof der evangelischen Kirchengemeinde St. Georg/Genin in Lübeck sollen keine anonymen Bestattungen mehr zulässig sein; für jedes Grab soll wenigsten ein Namensschild verpflichtend sein, wie die Vorsitzende des Kirchengemeinderates Monika Paustian erläuterte: „Wir sind der Auffassung, dass Verstorbene über den Tod hinaus der Name bleiben sollte, als Menschen und Christen.“ Schon 2009 habe man daher beschlossen, nach Belegung des bisherigen Gräberfelds für anonyme Bestattungen kein weiteres derartiges Gräberfeld zu schaffen. Die Lübecker Pröpstin Petra Kallies rechtfertigt diese umstrittene Entscheidung: „´Ich habe Dich bei Deinem Namen gerufen, Du bist mein`, heißt es in der Bibel bei Jesaja 43, Vers 1. Jeder und jede einzelne wird von Gott gesehen.“ Diese Individualität höre für Christen nicht auf. Der Name auf dem Grab sei ein wichtiger Ausdruck des christlichen Glaubens: „Wir respektieren, wenn Menschen ihre Angehörigen anonym bestatten wollen, aber auf unseren Friedhöfen ist es nicht die Form, die wir wünschen.“

Franz-Helmut Pohlmann aus Heide, Obermeister der Bestattungsinnung Schleswig-Holstein, stellt dagegen einen gesellschaftlichen Wandel bei der letzten Ruhe der Menschen fest: „Früher war es selbstverständlich, dass die Großfamilie, bei der mehrere Generationen unter einem Dach lebten, in einem großen Familiengrab bestattet wurde.“ Heute gebe es oft niemanden mehr, der nach dem Tod eines Angehörigen die Grabpflege übernehmen wolle. Dadurch steige die Zahl anonymer Bestattungen. „Natürlich gibt es solche Bestattungen auch auf kirchlichen Friedhöfen. Diese können sie überhaupt nur da ablehnen, wo es parallel noch einen kommunalen Friedhof gibt.“ Der Vizepräsident des Kirchenamts der Evangelischen Kirche in Deutschland, Thies Gundlach, sieht keinen Anlass zum Streit: „Im Grundsatz ist es gut, wenn Menschen einen Ort des Trauerns haben, an dem der Name des Verstorbenen sichtbar wird. Deswegen empfehlen wir in der Seelsorge, Gräber mit Namen zu versehen. Wir haben die Erfahrung gemacht, dass Menschen, die keinen Ort mehr zum Trauern haben, oft hilfloser sind, als Menschen, die an einem Grab eines Verstorbenen gedenken können.“ Wenn Menschen allerdings partout anonym bestattet werden möchten, müsse auch die Kirche dies respektieren: „Der Eindruck, dass eine Bestattung mit einem Grabstein erwünscht ist, weil das dem Friedhofsträger mehr Geld in die Kasse bringt, sollte vermieden werden.“ Als Pastor wirkt er an anonymen Bestattungen mit; das gelte auch für Seebestattungen, wo es in der Natur der Sache liegt, dass es keinen Grabstein gibt: „Im Blick auf die Opfer von Schiffsunglücken und Katastrophen wäre alles andere auch seelsorgerisch nicht verantwortlich“ (Lassiwe, Ärger um die letzte Ruhe, Schleswig-Holstein am Sonntag, 23.08.2015, 6).

Datenschutznachrichten aus dem Ausland

Europa

Nur begrenzte Transparenz über Google-Löschungen

Mit Urteil vom 13.05.2014 hat der Europäische Gerichtshof (EuGH) entschieden, dass Suchmaschinen wie Google Links zu Inhalten aus ihren Ergebnislisten entfernen müssen, wenn ein Nutzer in seinen Persönlichkeitsrechten verletzt ist (C-131/12). Ein Spanier wollte über die Suchmaschine nicht mehr im Zusammenhang mit einer 15 Jahre alten Geschichte auffindbar sein. Der EuGH stärkt damit ein „Recht auf Vergessenwerden“, wobei der ursprüngliche Zeitungsartikel im Netz bleiben durfte. So sollen etwa falsche, irrelevante oder inaktuelle Informationen verborgen werden können, damit Menschen nicht ihr Leben lang von ihnen verfolgt werden.

Bis Juli 2015 waren bei Google rund 280.000 Anträge gestellt worden, um insgesamt mehr als eine Million Links zu löschen. In 41% der Fälle ist Google dem Ersuchen nachgekommen. Diese Zahlen nennt Google im eigenen Transparenzbericht, zusammen mit 22 exemplarischen Löschanfragen. Diese drastischen Fälle lassen leicht den Eindruck entstehen, dass vor allem Kriminelle oder zwielichtige Politiker das Recht auf Vergessenwerden nutzen, um ihr öffentliches Image aufzupolieren.

Journalistische Recherchen zeigen jedoch, dass die Realität etwas anders aussieht. Google selbst teilt mit, man habe „immer versucht, bei unseren Entscheidungen in Bezug auf das Recht auf Vergessen so transparent wie möglich zu sein“. Die Daten seien Teil eines Versuches gewesen, um herauszufinden, wie sich die Anfragen kategorisieren lassen.

Die Zuteilung sei aber nicht verlässlich genug gewesen, um sie zu veröffentlichen. Deshalb habe Google den Test im März 2015 abgebrochen. Derzeit arbeite man daran, den Transparenzbericht zu verbessern.

Gemäß den Recherchen stammen mehr als 95% der Anträge von normalen Nutzenden, die Links zu Inhalten mit privaten Informationen gelöscht haben wollen. Während knapp die Hälfte der „privaten oder persönlichen Informationen" gelöscht wird, lehnt Google rund zwei Drittel der Löschanfragen aus den Kategorien „politisch", „Persönlichkeit des öffentlichen Lebens" und „schwere Verbrechen" ab. Griechen und Bulgaren stellten nur rund 100 Anträge pro eine Million Einwohner, in Estland und Liechtenstein sind es zehnmal so viele. Deutschland liegt mit 458 Löschanfragen im Mittelfeld. In Italien sollten besonders häufig Links im Zusammenhang mit schweren Verbrechen entfernt werden (12% aller Anfragen), Rumänien führt die Liste bei den politischen Löschanträgen an (7%), und in Ungarn wollten viele Prominente ihre Informationen bei Google entfernen lassen (8%). In Deutschland machen diese Kategorien jeweils weniger als ein Prozent der Gesuche aus, 98% stehen im Zusammenhang mit privaten oder persönlichen Informationen.

Ein Experten-Beirat hatte einen Leitfaden für die Entfernung von Daten im Internet erstellt. Im Mai 2015 hatten 80 WissenschaftlerInnen in einem offenen Brief an Google mehr Transparenz beim Umgang mit Löschanfragen. Dem schloss sich im Juli 2015 die frühere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger an, die als Beraterin im „Löschbeirat" von Google sitzt. Sie kritisierte, dass Google entgegen der Empfehlung des Beirats bisher keinen Bericht über die Maßstäbe beim Entfernen von Links vorgelegt habe.

Der britische Vize-Datenschutzkommissar David Smith forderte in einer Anordnung vom August 2015, dass Google auch Links zu frischen Medienberichten über das Löschen von Links zu früheren Informationen entfernen müsse, weil in den neuen Artikeln die alten Vorwürfe gegen die Person wiederholt würden. Die Links sollen bei der Internetsuche nach dem Namen des Antragstellenden nicht angezeigt werden. Im konkreten Fall ging es um ein 10 Jahre zurückliegendes kriminelles Vergehen (SHZ am Sonntag 23.08.2015, Online S. 19, Hurtz, Schwamm drüber, SZ 16.07.2015, 25; Tippmann, Google's Data On the the Right to be Forgotten, http://sytpp.github.io/rtbf/index.html).

Europa

Steuerabkommen mit der Schweiz

Im Kampf gegen die grenzüberschreitende Steuerflucht haben die EU und die Schweiz ein Abkommen über den Austausch von Bankdaten besiegelt, das am 16.09.2015 vom Schweizer Nationalrat gegen den heftigen Widerstand der Schweizerischen Volkspartei (SVP) bestätigt wurde. Der für Steuern zuständige EU-Kommissar Pierre Moscovici hatte in Brüssel nach der Unterzeichnung des Abkommens am 27.05.2015 erklärt: „Es eröffnet eine neue Ära der Steuer-Transparenz und markiert de facto das Ende des Bankgeheimnisses für die EU und die Schweiz" . Der Austausch von Bankdaten soll im Jahr 2018 beginnen. Die EU-Staaten erhalten künftig von der Schweiz jährlich Daten zu jenen Steuerpflichtigen, die ein Schweizer Konto haben. Dazu gehören Namen, Adressen, Steuernummern und Geburtstage sowie Informationen zu Finanzen und Kontostand. Damit halten sich die beiden Partner laut Kommission an weltweite Standards der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) und der G 20. Diese vereint große Industrie- und Schwellenländer. 7 Jahre zuvor hatte der damalige Finanzminister der Schweiz Hans-Rudolf Merz noch erklärt: „An diesem Bankgeheimnis werdet ihr euch die Zähne ausbeißen, es steht nämlich nicht zur Disposition." Laut Moscovici ist nun eine neue Etappe erreicht. Die Kommission verhandelt derzeit ähnliche Abkommen mit Andorra, Liechtenstein, Monaco und San Marino aus. Sie sollen noch vor Ende des Jahres 2015 unterzeichnet werden (Schweiz kippt Bankgeheimnis, SZ 17.09.2015, 22; EU läutet das Ende des Bankgeheimnisses ein, www.welt.de 27.05.2015).

Europa

Bei Outdorkleidung Terrorismusverdacht

Aus einem vertraulichen Papier der Europäischen Kommission geht hervor, dass in den Schengen-Raum Einreisende aufgrund ihrer äußeren Erscheinung auf einen möglichen Terrorhintergrund überprüft werden. EU-Staatsangehörige, die aus Konfliktgebieten zurückkehren, werden auf sog. Risikoindikatoren hin untersucht, wozu Wunden, Verletzungen und Verbrennungen gehören. Geachtet werden soll zudem an den Schengen-Außengrenzen auf blasse Hautpartien, die auf eine frische Bartrasur schließen lassen, sowie Militär- und Outdoorkleidung. Als risikobehaftet gelten der Liste zufolge Männer im kampffähigen Alter mit einschlägigen Tätowierungen und nervösem Verhalten. Die Kommission listet insgesamt 25 Merkmale auf.

Bei Verdächtigen soll es einen Abgleich in den europäischen Polizeidatenbanken geben. Die Maßnahmen betreffen u. a. Reisende aus Bürgerkriegsstaaten wie Syrien oder dem Irak sowie aus deren Nachbarländern wie der Türkei oder Jordanien. Die Risikoindikatoren sind in Brüssel umstritten. KritikerInnen fürchten eine systematische Personenkontrolle von EU-BürgerInnen im Schengen-Raum, der eigentlich einen weitgehend freien Personenverkehr garantiert (Outdoorkleidung macht verdächtig, Der Spiegel 29/2015, 13).

Europa/Deutschland

Außergerichtlicher Vergleich zwischen Google und Mosley

Der ehemalige Motorsport-Präsident Max Mosley und der Internetkonzern Google beendeten ihren langjährigen Rechtsstreit mit einer außergerichtlichen Vereinbarung, die diese am 11.05.2015 unterzeichneten, wie Tanja Irion, Mosleys Anwältin in Deutschland, bestätigte: „Der Streit ist beigelegt, zur Zufriedenheit beider Seiten." Über Details der Einigung haben Google und Mosley Stillschweigen vereinbart. „Die Vereinbarung ist vertraulich", sagte Mosley und

ergänzte: „Ich bin zufrieden und möchte sie nicht gefährden.“ Der Fall beschäftigte seit Jahren Gerichte in Deutschland, Frankreich und Großbritannien. Mosley hatte Google verklagt, weil sich der Suchmaschinenbetreiber weigerte, illegale Bilder einer privaten Sadomaso-Party Mosleys von vorneherein aus seinen Suchergebnissen herauszufiltern. Hunderte Webseitenbetreiber, die die Fotos immer wieder hochladen, hat Mosley bereits erfolgreich verklagt, weil sie seine Persönlichkeitsrechte verletzten. Ein britisches Boulevardblatt hatte Mosley 2008 heimlich bei einer privaten Sex-Party gefilmt und das Video ins Netz gestellt. Ein Gericht in Paris sowie das Landgericht Hamburg hatten Google bereits in erster Instanz verpflichtet, diverse Fotos aus seinen Treffern herauszufiltern (DANA 1/2014, 49). Das Oberlandesgericht Hamburg sollte am 19.05.2015 in dem Berufungsverfahren seine Entscheidung verkünden. Dies konnte Google durch die Vereinbarung verhindern.

2012 hatte Mosley noch gemeint: „Es geht nicht mehr um mich. Ich habe Zeit und Geld. Wenn man beides hat, ist man verpflichtet zu kämpfen, damit es anderen nicht genauso ergeht.“ Google wiederum hatte argumentiert, man wolle sich nicht zum Zensor des Netzes machen. Einen technischen Filter zu bauen sei ein unzumutbarer Aufwand und zugleich ein Präzendenzfall, der zahllose Promis, Politiker und Unternehmen auf den Plan rufen würde. Der Streit hatte Mosley fast eine Million Euro gekostet. Google hatte anscheinend erkannt, dass es juristisch keine Chance hatte, insbesondere nachdem der EuGH am 13.05.2014 gegen Google ein „Recht auf Vergessenwerden“ judizierte. Mit einer weiteren rechtlichen Niederlage wäre für Google ein weiterer Imageverlust verbunden gewesen (Hülsen, Der Spiegel 21/2015, 72).

Frankreich

Mitarbeiter-Scan über soziale Medien

Drei französische Wissenschaftler wollten mit einem Experiment herauszufinden, in welchem Umfang Firmen soziale Medien wirklich nutzen. Das Ergebnis, das sie am 11.08.2015 auf Jahrestagung des Ökonomenvereins „European Economic Association“ (EEA) in Mannheim vorstellten, ist aufschlussreich für Stellenbewerbende. Serge Pajak und zwei andere Ökonomen von der Uni Paris Süd bewarben sich für ihre Studie mehr als ein Jahr lang unter zwei fiktiven Namen bei französischen Firmen. Dabei verschickten sie für beide Scheinkandidaten identische Unterlagen, die völlig identische Fähigkeiten für den Job zeigten. Der einzige Unterschied zwischen den Bewerbenden: Im Netz konnte die Firma bei den Kandidaten eine Abweichung finden, wenn sie sich die Facebook-Profile ansah: Der eine Bewerber war demnach in Marokko geboren, nicht in Frankreich wie der andere. Das Ergebnis war eindeutig: Der angebliche Marokkaner wurde in 13% aller Fälle zu einem Bewerbungsgespräch eingeladen. Der angebliche Franzose dagegen in 21% aller Fälle.

Aus den Ergebnissen des Experimentes lässt sich erkennen, dass Firmen tatsächlich Daten über Bewerbende in sozialen Medien scannen, anders, als sie es oft behaupten. Zudem muss der Schluss gezogen werden, dass Arbeitgeber Bewerber aufgrund von Merkmalen wie ihrer Herkunft diskriminieren. Das ist ebenso wie die Diskriminierung etwa wegen des Geschlechts in vielen Ländern verboten - es wird aber praktiziert, wie die Studie nahelegt. Einen weiteren Beleg für ihre Erkenntnisse erhielten die Forscher, als Facebook das Design der Profilseiten veränderte. Auf einmal rutschte die Information über den Geburtsort auf eine Untersektion der Hauptseite, die man erst anklicken musste. Prompt erhielt der angebliche Marokkaner, der nicht mehr auf den ersten Blick als solcher zu erkennen war, mehr Einladungen. Wie schützen sich Bewerber vor solchen Diskriminierungen? Der Rat liegt auf der Hand: Indem sie weniger über sich im Netz preisgeben, um nicht nackt auf Facebook zu sein (Hagelüken, Nackt durch Facebook, SZ 16.08.2015, 17).

Belgien

Diskussion über Flüchtlings-Kennzeichnung

Der belgische Innenminister Jan Jambon von der flämisch-nationalistischen N-VA hat mit seinem im Rundfunk gemachten Vorschlag Wirbel ausgelöst, alle Asylsuchenden sollten ein Kennzeichen tragen, auf dem Name, Foto und Adresse ihres Flüchtlingsheims verzeichnet sind. Bei Polizeikontrollen seien sie damit schneller zu identifizieren. MenschenrechtlerInnen protestierten umgehend. Die Opposition sprach von „Stigmatisierung, die an die schlimmsten Perioden der Geschichte erinnert“. Jambons Ministerium präzisierte später, es handele sich keineswegs um einen „Badge“, den Flüchtlinge um den Hals tragen oder am Körper befestigen müssten. Das Ganze sei freiwillig und solle den Betroffenen das Leben nur erleichtern (Kennzeichen für Flüchtlinge, SZ 29.10.2015, 8).

Italien, weltweit

Spähsoftware-Export durch Hacking Team

- Leak

Anfang Juli 2015 stellte ein Unbekannter rund 400 Gigabyte interner Unterlagen der italienischen Firma „Hacking Team“ ins Internet, darunter Dokumente, E-Mails, Verträge und sogar Teile des Programmcodes der Hacking-Team-Spähsoftware. Auch das Twitter-Konto der Firma hatte der Unbekannte übernommen und machte darüber öffentlich, dass er die Interna der Firma geraubt hatte. Hacking Team hat den Trojaner „Remote Control System“ programmiert, mit dem u. a. Zielpersonen für die kurdische Autonomiebehörde im Nordirak überwacht werden. Das Programm sorgt für die komplette Überwachung der infiltrierten Smartphones und Computer. Die Software überwindet Verschlüsselung und kann Handys in Wanzen verwandeln. Sie hilft Strafverfolgern beim Überführen von Schwerstkriminellen, ist aber zugleich auch ein mächtiges Instrument auf einem kaum zu kontrollierenden Markt. Der Chef des Geheimdienstes von Zypern musste zurücktreten, weil die veröffentlichten Dokumente zeigen, dass seine Behörde Hacking-Team-Software nutzte, deren Einsatz nach zypriotischem Recht illegal ist. Auch in Deutschland dürften die

Polizeibehörden die Software nur unter engen Voraussetzungen einsetzen.

In einem Schulungsdokument für Vertriebsmitarbeiter heißt es ausdrücklich: „Gehe nicht auf die Hacking Team Website“. Das Demo Kit, mit dem die Fähigkeiten des Trojaners zukünftigen Kunden in aller Welt präsentiert werden sollen, habe mit Absicht nirgends das Logo der Firma aufgedruckt. Im Handbuch steht, dass die Hacking Team Software selbst keine Spuren verursache, „keine Vibration, kein Geräusch oder grafischen Effekt“. Nichts soll Rückschlüsse auf die Firma zulassen.

Aus den Unterlagen zeigt sich eine geschäftliche Dreiecksbeziehung zwischen Programmierern von Hacking Team in Italien, Kunden und Überwachern im Irak und einem Dienstleister in Deutschland. Im Städtchen Lebach im Landkreis Saarlouis koordiniert Simon T. als technischer Supporter das Ausspähen für Hacking Team und kann darüber Tastaturanschläge, Webseitenaufrufe, Passworteingaben der überwachten Geräte nachvollziehen. Die Software der Firma Hacking Team ist ohne technischen Support nicht oder nur sehr kurze Zeit nutzbar.

- Exportkontrolle

Als die Bundesregierung im September 2014 die Peshmerga-Kämpfer mit Waffen für den Kampf gegen den Islamischen Staat (IS) ausstattete, war damit eine Kursänderung in der deutschen Außenpolitik verbunden. Die kurdische Autonomiebehörde hatte schon 2010 digitales Rüstzeug aus Deutschland erhalten: Die deutsche Firma Intech-Solutions mit Sitz in Neufahrn bei Freising lieferte 2010 den Hacking-Team-Trojaner an das „Security and Intelligence Department“ in Arbil, für die Simon T. als freier Mitarbeiter arbeitet. 2015 wurde der Vertrag mit der kurdischen Regionalregierung um ein weiteres Jahr verlängert. Insgesamt haben sie bisher rund 500.000 Euro in die Überwachung investiert.

Experten schätzen den Markt für Überwachungstechnologie auf mehr als fünf Milliarden US-Dollar jährlich. Ungefähr ein Dutzend Firmen weltweit stellt sogenannte offensive Spähsoftware her, die tief in die Rechner von Überwachungszielen eindringt. Der kleine und äußerst lukrativen Markt staatlicher Überwachung war bis Anfang 2015 weitgehend unreguliert. In Deutschland gab es außer einem Exportverbot für Syrien und Iran keine gesetzlichen Beschränkungen für die Ausfuhr von Spähsoftware. Die Bundesregierung hatte sogar Exportbürgschaften für einzelne Firmen übernommen. Bundeswirtschaftsminister Sigmar Gabriel verfügte dann aber 2014 durch Einzeleingriffe einen faktischen Exportstopp. Seit Januar 2015 gilt zudem eine EU-Verordnung, gemäß der Spähsoftware gemäß dem Wassenaar-Abkommen für Exportkontrollen als Dual-Use-Gut eingestuft wird. Die Ausfuhr von Spähsoftware außerhalb der EU ist nun genehmigungspflichtig. Am 09.07.2015 führte die Bundesregierung zusätzliche Änderungen in der Außenwirtschaftsverordnung ein, wonach auch die technische Unterstützung von Spähsoftware kontrolliert werden soll.

Die Ausfuhr der Software in den Irak wurde bis Anfang 2015 von keiner Behörde kontrolliert. Hacking-Team-Sprecher Eric Rabe teilte mit, dass man nun eine „globale“ Ausfuhrgenehmigung habe. Das italienische Ministerium für wirtschaftliche Zusammenarbeit bestätigte, allerdings ohne diese zu spezifizieren, dass es eine Genehmigung für „nicht sensitive Länder“ gebe.

- Kooperation mit Diktatoren

Schon seit Jahren kritisieren Menschenrechtsgruppen, dass Hacking Team ihre Spähsoftware auch an repressive und diktatorische Regime verkauft, was die Firma bislang bestritt. Sprecher Eric Rabe erklärte nach der Veröffentlichung der Unterlagen, man habe „keine Gesetze gebrochen“ und sich „komplett ethisch verhalten“. Die Firma sieht sich als Dienstleister der Guten. In dem Leak finden sich allerdings Verträge mit Geheimdiensten und Polizeibehörden aus Ländern wie Ägypten, Äthiopien, Honduras, Russland und Kasachstan. In diesen Staaten können regimekritische Äußerungen ein Verbrechen sein. Die Hacking-Team-Trojaner können so auch zum Ausspähen von Computern und Telefonen von Demokratieaktivisten eingesetzt werden, was das Hacking Team offenbar bewusst in Kauf nahm. Ein Hacking-Team-Mitarbeiter kommentierte 2012 ironisch die Vorwürfe bahrainischer Aktivisten gegen den deutschen Konkurrenten Finfisher, dass dessen Software gezielt zur Ausspähung der Demokratiebewegung genutzt werde, mit „Eine gute Geschäftsgelegenheit in Bahrain“. 2013 kaufte das Bahrainische Verteidigungsministerium dann tatsächlich in Mailand ein, Hacking Team berechnete 210.000 €.

- Das Unternehmen

Die 2003 gegründete Firma in Mailand, an der die italienische Region Lombardei zu 26% beteiligt ist, hatte zunächst geholfen, anderen die eigene IT-Infrastruktur zu sichern, indem sie die Systeme ihrer Kunden hackten, um die Schwachstellen herauszufinden. Unter den Kunden sind große Namen wie etwa die Allianz. Aus den geleakten Abrechnungen ergibt sich, dass die Firma sich wohl seit 2011 auf das lukrativere Geschäft mit der staatlichen Angriffssoftware spezialisierte. Hacking Team avancierte schnell zu einem wichtigen Akteur mit einem Jahresumsatz von 7,73 Millionen € im Jahr 2014.

Geschäftsführer David Vincenzetti schrieb in einer Email von 2012, als Kunden verunsichert auf die anhaltende Kritik an dem sogenannten Bundestrojaner in Deutschland reagieren: „Ihr habt es hier mit dem Ferrari der Cyberangriffe zu tun“. Im Februar 2015 schrieb er: „Wir sind sicher berüchtigt, vielleicht der berüchtigste Name im Markt der Angriffssoftware. Das ist großartig“. Sich selbst bezeichnet er einmal als „Kriegsmaschine, arbeitsmäßig“. Gemäß dem Leak beobachtet David Vincenzetti die Weltlage genau. Er hatte Artikel der „New York Times“ abonniert und einen Filter für die Worte „Nuklear“ und „Folter“ eingerichtet. Berichte, die er für besonders interessant hielt, schickte er an seine Mitarbeiter weiter. Einen Artikel über Saudi Arabiens hartes Durchgreifen gegenüber liberaleren Kräften leitet er als „absolute Leseempfehlung“ weiter, „gerade weil Saudi eine lokale Supermacht (und ein sehr wichtiger Kunde von uns) ist“.

Als im Iran 2011 Demonstrationen durch die Straßen Teherans ziehen, verabredete sich ein Hacking-Team-Mitar-

beiter mit einem Vertreter der iranischen Telekommunikationsgesellschaft TCT zu einem „privaten Treffen“, um den Hacking-Team-Trojaner vorzustellen, der auch „Skype und MSN Chats“ abfangen kann. Sprecher Eric Rabe gab an, Iran sei nie ein Kunde der Firma gewesen. 2014 wurden die Vereinten Nationen (UN) auf einen Deal von Hacking Team mit dem sudanesischen Geheimdienst aufmerksam. Der Sudan ist seit 2005 strengstens sanktioniert. Dennoch verkaufte Hacking Team 2012 seinen Trojaner für 869.000 Euro an den Staat. Die UN kommt in einem Brief vom März 2015 zu der Bewertung, die Software sei ideal dazu geeignet, bei militärischer Aufklärung zu helfen: „Sie könnte in die Kategorie Militärische Ausrüstung oder Unterstützung fallen.“ Gemäß Sprecher Rabe ist der Sudan heute kein Kunde mehr.

Auch die Schweiz, Polen und die USA beziehen Überwachungssoftware aus Mailand. Der luxemburgische Geheimdienst wird, als Steuerbehörde getarnt, seit 2012 als Kunde betreut - ebenfalls von Simon T. im Saarland. Sogar Beamte des Bundeskriminalamts (BKA) und der Landespolizei Bayern besuchten die Firma im März 2011 und im Januar 2012, um sich den RCS Trojaner vorführen zu lassen.

Wenige Wochen nach dem Besuch erbat ein Techniker des BKA Hilfe für einen „speziellen Fall“. Man benötige einen Keylogger für einen Mac-OSX Computer: „Haben Sie ein Produkt, das unseren Bedürfnissen entspricht?“ Ob Hacking Team ein Angebot machte, lässt sich nicht nachvollziehen. Eine BKA-Sprecherin erklärte: „Im BKA finden keine Softwareprodukte der Firma Hacking Team Anwendung.“

Eine E-Mail von Simon T. zeigt, dass andere Firmen vorsichtiger sind: Der Versuch, die französische Konkurrenzfirma Vupen als neuen Lieferanten zu gewinnen scheiterte, weil diese sich weigerte, in den Irak zu exportieren. Auch Hacking Team Mitarbeiter sorgen sich mittlerweile, gemäß einer Mail, um die Region: Der „Islamische Staat“ stehe 20 Kilometer vor Arbil: „Es wäre hilfreich zu verstehen, wie die Situation mit Simon und dem Kunden Condor ist, und wie wir verhindern, dass die Installation in die falschen Hände gerät. Um uns zu schützen und auch den Kunden.“ David Vincenzetti sah allerdings eher die Geschäftschancen, als er in einem weiteren E-Mail-Austausch schrieb, Hacking Team sei bereits autorisiert, an die irakische Regierung zu liefern: „Sie werden Cybertechnologien bald sehr nötig haben, um die Terroristen zu bekämpfen. Let‘s kick some ass!“ (Kampf/Spinrath/Strozyk/Tandriverdi, Deutsche Firmen koordinieren Späh-Angriffe, www.sueddeutsche.de 15.07.2015; diess., Außer Kontrolle, SZ 16.07.2015, 17).

Großbritannien

„Sun“-Reporter wegen Datenbeschaffung bestraft

Ein Reporter des Boulevardblatts „Sun“ wurde für den Kauf vertraulicher Informationen bei einem Polizisten einer Anti-Terror-Einheit am Londoner Flughafen zu einer Freiheitsstrafe von 18 Monaten auf Bewährung wegen Beihilfe und Anstiftung zum Amtsmissbrauch verurteilt („Sun“-Reporter verurteilt, SZ 30./31.05.2015, 46).

Schweden

Bei Klarna wird nach Lieferung bezahlt

Niklas Adalberth und Sebastian Siemiatkowski haben in Schweden einen Bezahldienst „Klarna“ aufgebaut, bei dem Kunden ihre Waren erhalten, bevor sie zahlen. Mitgeliefert wird eine Rechnung, die sie innerhalb von 14 Tagen begleichen müssen - bei Klarna, nicht beim Händler. Das Start-up übernimmt gegen Gebühr dessen Risiko, dass einer nicht bezahlt. Etwa 50.000 Händler arbeiten weltweit mit Klarna zusammen. Fünf Millionen Menschen in Schweden nutzen laut Adalberth den Dienst, 40% aller Online-Zahlungen liefen über Klarna. In Deutschland, wo gut achtmal mehr Menschen leben, sind es nach eigenen Angaben rund 25 Millionen Nutzende. Klarna hat heute 1.300 Mitarbeitende und einen Jahresumsatz von 240 Millionen Euro.

Die beiden studierten mit einem weiteren Freund an der Stockholm School of Economics und nutzten zu dritt das Gründerzentrum der Uni, um die Idee mit dem Bezahldienst zu entwickeln und Investoren vorzustellen. 2004 traten die Firmengründer an der Uni bei einem Start-up-Wettbewerb an. Die Jury, in der Vertreter wichtiger Unternehmen der schwedischen Wirtschaft vertreten waren, zeigte sich, so Adalberth, wenig beeindruckt: „Sie haben gesagt: Ihr scheint ja ganz nette Jungs zu sein, aber macht lieber etwas anderes. Damit habt ihr keine Chance.“ 2005 gründeten sie trotzdem Klarna.

Inzwischen gibt es den Bezahldienst in 18 Ländern, seit 2010 in Deutschland. Der Start war holprig, Verbraucher klagten, dass Mahnungen zu früh und ohne Vorwarnung kamen - und mit ihnen eine Gebühr von derzeit 4,95 Euro. Früher war sie noch höher. In den Verbraucherforen häuften sich die Beschwerden. Inzwischen können Kaufende die Zahlungsfrist kostenlos um zehn Tage verschieben und erhalten eine Erinnerungsmail, zwei Tage bevor sie ausläuft. Für viele Händler in Schweden übernimmt Klarna inzwischen den gesamten Bezahlvorgang, nicht mehr nur die Option, auf Rechnung zu kaufen. Check-out-Service heißt das, die virtuelle Kasse: Der Kunde sucht Waren im Internet aus, klickt auf „Kaufen“ und kann dann entscheiden, ob er per Kreditkarte, Überweisung, Ratenkauf oder Lastschrift zahlen möchte. Wählt er nichts aus, bekommt er automatisch eine Rechnung. Wenn Klarna hinter diesem Check-out steht, zahlt er immer an Klarna - egal auf welchem Weg.

Klarna nimmt eine Bonitätsprüfung vor und nutzt hierfür Auskunfteien wie die Schufa, sowie 139 weitere Variablen. Wenn jemand um drei Uhr nachts einkauft, ist es, so Adalberth, beispielsweise wahrscheinlicher, dass er nicht bezahlen wird als um drei Uhr nachmittags. Klarna entscheidet so über bis zu 300.000 Transaktionen am Tag. Wer als nicht kreditwürdig eingestuft wird, muss vor Lieferung zahlen. Die Kaufenden bekommen in der Regel von diesen Berechnungen nichts mit. Der Kaufvorgang ist einfach gestaltet. Wer z. B. bei einem Online-Buchhändler ein Buch kaufen möchte, klickt auf „kaufen“. Damit ist die Bestellung abgeschlossen, weitere Angaben sind nicht notwendig.

Sobald das Buch verschickt ist, taucht es im Klarna-Account auf. Dort sind alle offenen Rechnungen aufgelistet, inklusive Preis und Fälligkeit. Klickt er hier auf „bezahlen“, wird das Geld sofort überwiesen. Pin oder Kontonummer müssen nicht angegeben werden, wenn zuvor das Bankkonto online mit Klarna verbunden worden ist. Soweit ist das System in Deutschland allerdings noch nicht (Bigalke, Aus Trotz zum Erfolg, SZ 31.08.2015, 22).

Israel

Videoüberwachung soll Frieden auf den Tempelberg bringen

Ein konkretes Ergebnis der Krisengespräche in der jordanischen Hauptstadt Ammann am 24.10.2015 bei der Vermittlungsmission des US-Außenministers John Kerry im Nahen Osten ist die Einführung eines umfassenden Videoüberwachungssysstems auf dem Tempelberg in Jerusalem. Eine Welle der Gewalt hatte bis dahin allein im Oktober 2015 mehr als 60 Tote gefordert. Kerry: „Die ganze Gewalt und die Anstiftung zu Gewalt müssen aufhören.“ Kerry hatte zunächst mit Israels Premierminister Benjamin Netanjahu und dann mit dem jordanischen König Abdullah II sowie mit Palästinenser-Präsident Mahmud Abbas verhandelt. Natanjahu stimmt dem „exzellenten Vorschlag“ des jordanischen Monarchen zu, das Gelände, das die Muslime Haram al-Scharif nennen und auf dem sich die islamischen Heiligtümer Al-Aksa-Moschee und Felsendom befinden, rund um die Uhr zu überwachen.

Kerry hofft, dass mit diesem „game changer“ die Wende kommen könnte. Netanjahu bestätigte, dass sich die israelische Grundhaltung nicht verändert habe: „Muslime beten auf dem Tempelberg. Nicht-Muslime besuchen den Tempelberg.“ Vorausgegangen waren zwei Offensiven auf dem Tempelberg, der Muslimen wie Juden gleichermaßen heilig ist: Radikale jüdische Gruppierungen zeigten verstärkt Flagge und verstießen offen gegen das vereinbarte Gebetsverbot für Nicht-Muslime. Auf palästinensischer Seite wurde dies als Provokation verstanden und war Anlass für die Mobilisierung für den „Kampf um Al-Aksa“. Nach der Einigung über die verstärkte Kontrolle haben jüdische Tempelberg-Aktivisten sogleich dazu aufgerufen, jetzt erst recht in Massen dorthin zu strömen. Die Palästinenser bleiben skeptisch und fürchten, dass die Kameras nur zu neuen Festnahmen führen. Die Revolte wird auf beiden Seiten von jugendlichen EinzeltäterInnen getragen, die schwer zu kontrollieren und zu beeinflussen sind. Zudem trat der „Islamische Staat“ (IS) mit einem Video auf den Plan, in dem ein maskierter Kämpfer auf Hebräisch droht, die IS-Milizen würden „die Al-Aksa-Moschee als Eroberer betreten“ und es bleibe „bald kein Jude mehr in Jerusalem übrig“ (Münch, Kameras als Friedensbringer, SZ 26.10.2015, 7).

USA

Röntgen-Vans in New York

In New York sind Kleintransporter der Polizei unterwegs, die innen mit Röntgenstrahlern und einem eigenen Generator ausgestattet sind. Diese Transporter sind in der Lage, durch Häuserwände, durch Kleidung von PassantInnen und in fremde Fahrzeuge hineinzuschauen. Auf Anfrage der Bürgerrechtsorganisation Civil Liberties Union (ACLU) erklärte New Yorks Polizeichef William Bratton offensichtlich ziemlich genervt, so etwas mache sie natürlich nicht. Jeder, der behaupte, dass die Polizei ihre Röntgenmobile nicht gesetzestreu verwende, könne ja vor Gericht ziehen: „Und sie werden verlieren!“.

Die 800.000 Dollar teuren Transporter, Modell Mercedes-Benz Sprinter, waren zuvor – soweit bekannt – vom US-Militär im Irak eingesetzt worden. Mit ihrer Hilfe sollten Waffendepots und Bombenlager enttarnt werden. In einem Werbeclip der Herstellerfirma lobt diese ihre „beispiellose Technik“. Der US-amerikanische Zoll setzt diese Geräte auch ein, um Schmugglern das Handwerk zu legen. Eine befriedigende Antwort, wofür diese Vans vom New York Police Department (NYPD) genutzt werden, gibt es bisher nicht. Auf diese Frage antwortete Bratton nur, sie würden nicht dazu eingesetzt, Menschen auf Waffen hin abzusuchen: „Ich werde absolut nichts sagen.“ 2013 hatte sich Bratton noch als Freund der Transparenz geriert: „Das NYPD sollte keine Geheimnisse haben.“ Schon 2011 hatte der US-Journalist Michael Grabell Fragen zu den Transportern gestellt: „Ich wollte einfache Dinge wissen: Für was genau diese Transporter benutzt werden, ob es Studien gab hinsichtlich gesundheitlicher Risiken und wie die Verträge zustande gekommen sind.“ Trotz Berufung auf das Informationsfreiheitsgesetz blockiert die Behörde jede Auskunft und die Vorlage der Dokumente mit der Begründung, dass die Informationen auch Terroristen interessieren könnten. Eine Richterin des Obersten Gerichts des Bundesstaates New York ordnete 2014 an, dass die angeforderten Dokumente zu übergeben sind: „Das hier ist eine Demokratie mit einer transparenten Regierung.“ Der Einsatz der Röntgen-Vans könne zudem signifikante Risiken für die Gesundheit mit sich bringen, so das Urteil: „Das NYPD bestreitet diesen Punkt nicht.“

Der Röntgen-Van setzt eine Technik ein, bei der Geräte und Körper ionisierender Röntgenstrahlen ausgesetzt werden. Diese können dazu führen, dass die Gene mutieren und sich z. B. Krebs bildet, auch schon, wie angeblich hier, bei geringer Dosis. Grabell wartet immer noch auf die Herausgabe der Dokumente. Es ist nicht einmal bekannt, wie lange die Röntgen-Vans schon im Einsatz sind. In einem 2007 erschienenen Buch über die Arbeit polizeilicher Bombensucher wird ein New-York-Besuch des damaligen Präsidenten George W. Busch im Jahr 2004 erwähnt. Dort wird beschrieben, dass Autofahrer bei einer Sicherheitskontrolle ihre Fahrzeuge im Schritttempo zwischen zwei Transportern hätten fahren müssen (Tandriverdi, Supergeheim, SZ 28.10.2015, S. 10).

USA

Bauarbeiterüberwachung per Drohnen

Beim Bau des Sportstadions in Sacramento/Kalifornien schwirren einmal täglich mehrere Drohnen über die Baustelle. Mit dem so gesammelten Video-

material wird am Computer eine dreidimensionale Darstellung vorgenommen, die über eine spezielle Software mit ebenfalls digitalisierten Plänen der Architekten abgeglichen wird. Fällt ein Abschnitt hinter das Soll zurück, gibt die Software eine Warnung aus. Das von US-Wissenschaftlern und einer japanischen Baufirma entwickelte Computerprogramm soll den Überblick und das Einhalten der Terminplanung sicherstellen. Erfasst wird auch die individuelle Arbeitsleistung der Bauarbeiter.

In Deutschland wären derartige Baustellenkontrollen mit individueller Leistungskontrolle nur unter engen Voraussetzungen zulässig. Doch der Düsseldorfer Arbeitsrechtsanwalt Peter Kaumanns kennt den Fall eines deutschen Hausbesitzers, der an seiner Pool-Baustelle eine Kamera installierte, um im Urlaub aus der Ferne den Fortschritt kontrollieren zu können. In einem anderen Fall habe ihm ein Bauherr in Frankfurt vorgeführt, wie die an einem sechs Meter hohen Mast montierte Webcam Bilder lieferte, auf denen die zehn bis zwanzig Bauarbeiter gut erkennbar waren. Zwar sei es dabei um den „Showeffekt" gegangen, also darum, den Käufern der dort entstehenden Luxuswohnungen im Zeitraffer vorzuführen, was bis zum Einzug so alles passiert. Dennoch habe ihm das Bauchschmerzen bereitet. Der Anwalt meinte: „Datenschutz ist noch immer ein stumpfes Schwert." Er kenne einige Unternehmen, die bedenkliche Methoden zur Kontrolle der Mitarbeiter einsetzen - und damit rechnen, dass der Verstoß ohnehin kaum geahndet wird (Bernau, Neue Luftmasche, SZ 02.03.2015).

USA

Taschenkontrollen bei Apple außerhalb der Arbeitszeit

Angestellte von Apple-Geschäften im US-Bundesstaat Kalifornien sind mit einer Klage gegen den Konzern gescheitert, rückwirkend die Durchsuchungen ihrer Taschen und die damit verbundene Wartezeit als Arbeitszeit vergütet zu bekommen. US-Bezirksrichter William Alsup wies eine Sammelklage von Beschäftigten am 07.11.2015 zurück: Es stehe ihnen frei, mit oder ohne Tasche zur Arbeit zu kommen. Apple hätte ihnen auch verbieten können, überhaupt eine Tasche mit zur Arbeit zu bringen. Die Beschäftigten in Apple-Geschäften müssen beim Verlassen ihres Arbeitsplatzes ihre Taschen durchsuchen lassen (Apple-Mitarbeiter gescheitert, SZ 09.11.2015, 22).

USA

KünstlerInnen-Ranking im Internet

Der 28jährige Internet-Dienstleister Carlos Rivera hat Februar 2014 eine Internetseite „Art Rank" eingerichtet, in der er Gegenwartskünstler nach ihrem Marktwert einstuft und auf einer Rankingliste präsentiert nach Kategorien wie „Jetzt Kaufen" (für weniger als 10.000, 30.000 oder 100.000 $), „Jetzt Verkaufen" oder „Kommender Klassiker". Vierteljährlich wird auf der Webseite gelistet, wer zukünftig in der Kunstszene boomen könnte und wer möglicherweise an Wert verliert. Bis zu 10 AbonnentInnen erhalten für 3.500 $ im Quartal die Kaufempfehlung schon Wochen bevor sie auf der allgemein zugänglichen Seite veröffentlicht werden. Rivera behauptet, wer in den vergangenen 16 Monate alle Empfehlungen beherzigt habe, hätte eine Rendite von 4.200% eingefahren.

Das kontroverse Ranking wird mit einem Algorithmus ermittelt. Grundlage der Berechnung sind zurückliegende Verkaufszahlen, Nennungen in Zeitungen, zukünftige Ausstellungen und Daten aus sozialen Netzwerken. Rivera verteidigt sein Vorgehen: „Personen zu ranken ist nichts Neues. Schauen Sie auf die Oscars oder auf Athleten".

KritikerInnen werfen Rivera vor, mit seiner Seite kaltherzige Kunstspekulation zu befeuern. Der langfristige Wert von Kunst lasse sich nicht mit einem Algorithmus bestimmen. Ob eine KünstlerIn in 10 oder 20 Jahren erfolgreich ist, hänge z. B. nicht davon ab, wie oft Werke in sozialen Netzwerken geteilt werden. Dem hält Rivera entgegen: „Ich kann auch nicht sagen, ob Kunst gut oder schlecht ist; ich kann nur beurteilen, was derzeit der Marktwert dafür ist". Sein Ziel sei es, mittels der prognostizierten Marktentwicklungen den Kunstmarkt transparenter zu gestalten: „Es gibt viele, die nicht wissen, wie man in diesen Markt einsteigt und wann man wieder aussteigen sollte." Einige Jahre zuvor war Rivera ein kleiner Galerist, der in West Hollywood unter dem Namen Rivera&Rivera „ineffizient" Fotografien verkaufte: „Es sind immer viele gekommen, aber die wenigsten haben etwas gekauft." Ende 2012 schloss Rivera, der zuvor Film und Betriebswirtschaftslehre an der University of Southern California in Los Angeles studiert hatte, die Galerie. Mit Rivera arbeiten ein Datenanalyst und ein Finanzexperte an „Art Rank", die am Anfang noch „Sellyoulater" hieß (Schinkels, SZ 03.09.2015, 13).

Saudi-Arabien

Verlobte wollen Transparenz über künftigen Gatten

Mehrere Klägerinnen aus der Stadt Abha fordern vor Gericht, dass der zuständige Scheich Einsicht in Polizei- und Krankenakten über den Bräutigam erhält und diese Informationen an die Braut weitergeben kann, bevor diese in den Ehevertrag einwilligt. Die Familienanwältin Najwa Salah meinte, die Kenntnis der persönlichen Biografie könne zu einer Senkung der Scheidungsrate im Land beitragen. Es gehe nicht darum, „jedes Detail aus der Vergangenheit" ihres Zukünftigen zu erforschen. Männer könnten frühere Fehler bereut haben. Viele Frauen erleben nach der Trauung aber Überraschungen, wenn sie die Geschichte ihres Vermählten näher kennenlernen. Gegen die rechtliche Forderung wird von Ahmed Al-Muabbi, Mitglied der Schiedsgerichte in Saudi-Arabien, eingewandt, auch durch den Koran sei ein gewisser Schutz der Privatsphäre gewährt. Nachforschungen durch eine Verlobte könnten das Vertrauensverhältnis untergraben oder zu einer trügerischen Sicherheit führen. Lupenreine Akten müssten nicht automatisch be-

deuten, dass der Mann auch tatsächlich „gut“ sei. Eine Aktenprüfung könne Männer demütigen und ihrem Selbstwert schaden. Frauen sollten aber durchaus erfahren, ob der Zukünftige schon einmal verheiratet war (Saudische Verlobte wollen gläserne Gatten, SZ 15.05.2015, 10).

Ägypten

Polizeistaatsregelungen im „Anti-Terror-Gesetz“

Der Präsident Ägyptens Abdel Fattah al-Sisi hat per Dekret ein neues sog. Anti-Terror-Gesetz mit 54 Artikeln in Kraft gesetzt. Für die Gründung und das Anführen einer terroristischen Gruppierung ist die Todesstrafe oder lebenslange Haft vorgesehen. Die Finanzierung von Attentaten wird mit lebenslanger Haft bestraft. Die Mitgliedschaft in einer solchen Vereinigung kann mit bis zu zehn Jahren Gefängnis geahndet werden, die Aufstachelung zur Gewalt, auch indirekt durch die „Verbreitung von Ideen, die zur Gewalt aufrufen“, mit fünf bis sieben Jahren. Die Tatbestände werden in dem neuen Gesetz sehr weit gefasst. Als Terrorismus werden künftig auch jegliche Angriffe auf staatliche Einrichtungen gewertet oder die Störung der öffentlichen Ordnung durch Gewalt oder Drohungen. Die Verbreitung von „Ideologien, die zur Gewalt anstacheln“, wird mit Haft bestraft.

Für Prozesse nach dem neuen Gesetz werden Sondergerichte eingerichtet, die schneller urteilen sollen; zudem werden die Rechtsmittel von Angeklagten eingeschränkt. Zugleich garantiert das neue Gesetz Angehörigen der Sicherheitskräfte Straffreiheit für die „verhältnismäßige Anwendung von Gewalt in Ausübung ihrer Pflichten“ im Kampf gegen den Terrorismus. Polizeigewalt und Folter sind in Ägypten verbreitet. In den wenigsten Fällen allerdings werden beschuldigte Beamte von der Justiz dafür zur Rechenschaft gezogen.

Ein Artikel des Gesetzes droht jedem Geldstrafen von umgerechnet 23.000 bis 57.500 €, der wissentlich Informationen über Terroranschläge und Anti-Terror-Operationen veröffentlicht, die den Angaben der Regierung widersprechen. Davon betroffen sind neben Journalisten auch Blogger, Menschenrechtler und möglicherweise Anwälte. Eine erste Fassung des Gesetzes, die nach dem Protest des ägyptischen Journalistensyndikats geändert worden war, sah noch Haftstrafen von mindestens zwei Jahren für solche Fälle vor. Weiterhin möglich sind Berufsverbote bei Verstößen gegen die Standards eines Berufs, ohne dass Journalisten explizit genannt werden. Solche Strafen sind für ägyptische Journalisten und kleine Medien existenzgefährdend. Präsident Sisi hatte das neue Gesetz Ende Juni 2015 nach dem tödlichen Anschlag auf Generalstaatsanwalt Hischam Barakat angekündigt. Menschenrechtler kritisieren weitreichende Einschnitte in Grundrechte. Nach Ansicht von Amnesty International und auch einiger ägyptischer JuristInnen und MenschenrechtlerInnen verstößt das Gesetz gegen die Verfassung von 2014 und gegen internationale Abkommen, die Ägypten ratifiziert hat. Die Bundesregierung sieht das Gesetz mit „großer Sorge“. Der Menschenrechtsbeauftragte Christoph Strässer sagte, Einschränkungen von Meinungs- und Pressefreiheit seien der falsche Weg, Terroristen den Nährboden zu entziehen. „Stabilität gibt es auf Dauer nicht ohne Grundrechte und den Respekt der Menschenrechte“ (Krüger, Weit gefasstes Gesetz, SZ 18.08.2015, 7).

Thailand

Lückenhafte Videoüberwachung

Viele Tage nach einem blutigen Bombenanschlag auf den Erewan-Schrein in Bangkok tappte die Polizei im Dunkeln. Bei dem Anschlag am 17.08.2015 in der thailändischen Hauptstadt waren 20 Menschen getötet worden, darunter 14 ausländische TouristInnen. Mehr als 120 Personen wurden verletzt. Polizeichef Somyot Poompanmoung gestand am 24.08.2015 ein, dass die Mehrzahl der Überwachungskameras in der Stadt zum Zeitpunkt des Anschlags nicht funktioniert habe, was die Suche nach den mutmaßlichen Tätern sehr erschwere: „Auf manch einer Straße gibt es vielleicht 20 Überwachungskamera, aber nur 5 funktionieren. Die anderen sind aus unerfindlichen Gründen kaputt.“ Zuvor hatte die Polizei eingestanden, dass ihr die nötige Technik für die Auswertung der Bilder fehle. Ungeachtet dieser und weiterer Ermittlungspannen wurden Mitte September ein Pakistaner sowie eine Frau und ein Mann aus Malaysia wegen des Bombenanschlags festgenommen (Lückenhafte Überwachung, SZ 25.08.2015, 8).

China

„Citizen Score“ schafft Freiheit

Die dominierenden chinesischen Online-Konzerne Alibaba und Tencent haben eine Anwendung aufgelegt, bei der für sozial erwünschtes Verhalten Punkte vergeben werden. Bei 350 geht es los; maximal zu erreichen sind 950. Von 600 Punkten an gibt es günstige Kredite und wird die Erteilung eines Visums erleichtert. Ab 700 Punkten darf man nach Singapur reisen; eine Reise nach Europa steht Nutzenden ab 750 Punkten offen. Die Punkte bei diesem „Citizen Score“ werden für Jubeläußerungen im Netz, erwünschte soziale Aktivitäten und richtiges Einkaufsverhalten gegeben. Punktabzüge gibt es für Kritik an der Kommunistischen Partei oder an sozialen und gesellschaftlichen Missständen. Die Daten kann jeder einsehen. In die Wertung fließt nicht nur das eigene Verhalten ein, sondern auch das von FreundInnen und Bekannten, mit denen man über soziale Medien verbunden ist. Noch ist das System freiwillig; von 2020 an soll es für alle, die einen chinesischen Pass besitzen, obligatorisch sein. In China ist das Angebot unbestritten. Der belgische Chinaexperte Rogier Creemers von der Oxford University vermutet, dass das System auf die vollständige Vermessung des Menschen abzielt. Es ähnelt den Überlegungen des Google-Stipendiaten Douglas Coupland, der Punkte verteilen will, mit denen Menschen sich Freiheitsrechte verdienen können (Punktrichter, FAZ 10.10.2015, S. 16).

Technik-Nachrichten

PIN-Ermittlung mit Wärmebildkamera

Mit Wärmebildaufnahmen der PIN-Pads von Geldautomaten oder Türschlössern können eingegebene Geheimzahlen identifiziert werden. IT-Sicherheitsforschende haben eine Technik entwickelt, wie sie selbst die Reihenfolge der Eingabe feststellen können. Bis zu eine Minute bleiben die betätigten Tasten wegen der über die Finger übertragenen Körperwärme für Wärmebildkameras sichtbar. Die IT-Sicherheitsexperten von Sec-Tec in Großbritannien warnen, dass diese Geräte mit knapp 300 Euro inzwischen so erschwinglich sind, dass sie sich praktisch jeder leisten kann. Kriminelle könnten mit Hilfe der Wärmebildaufnahmen die eingegebene PIN-Nummer über den Temperaturunterschied identifizieren und sich direkt auf ein Smartphone-Display übertragen lassen. Da viele solcher Geräte zur PIN-Eingabe über keine Sperre bei mehrfach falschen Eingaben verfügen, sei es möglich, die Reihenfolge der erkannten Tasten so lange auszuprobieren, bis der richtige Code eingegeben wurde. Eine Sprecherin des Bundesverbands deutsche Banken wies darauf hin, dass es bei dem vierstelligen von deutschen Banken verwendeten PIN-Code 24 Kombinationsmöglichkeiten gäbe, nach drei Fehlversuchen aber die Geheimzahl gesperrt werde. Die Forschenden bei Sec-Tec haben nach eigenen Angaben zwei verschiedene Methoden entwickelt, die Reihenfolge aus den Wärmebildaufnahmen zu errechnen, wobei sie aber Details hierzu verschweigen. Möglich ist eine hochdetaillierte Aufnahme, auf der Abstufungen in der verbleibenden Wärme auf den Tasten entweder sichtbar sind oder durch softwareseitige Auswertungen errechnet werden. In Kombination mit bereits bekannten Angriffen auf RFID-Chips ist es den IT-SicherheitsexpertInnen nach eigenen Angaben außerdem gelungen, die Zweifachauthentifizierung zu knacken, die bei elektronischen Türschlössern zum Einsatz kommt.

Die Abwehr solcher Angriffe ist relativ einfach. So können die Nutzenden nach Eingabe ihrer PIN ihre gesamte Handfläche kurz auf den Ziffernblock legen und so alle Tasten gleichermaßen aufwärmen. Die IT-SicherheitsexpertInnen empfehlen den Herstellern den Einsatz von PIN-Pads aus Metall, da der von ihnen getestete Angriff nur mit solchen aus Kunststoff oder Gummi funktioniere. Die Institute des Deutschen Sparkassen- und Giroverbands nutzen Metalltasten bei ihren Geldautomaten. David Wray von Sec-Tec teilte mit, er kenne noch keinen Fall, bei dem Kriminelle das Verfahren genutzt haben, um an Bankkonten zu gelangen: „Angesichts der Tatsache, dass die Technologie so günstig ist, ist zu erwarten, dass es in Zukunft solche Versuche geben wird“ (Güler, Warm, wärmer, am wärmsten, SZ 01.09.2015, 26; Wärmebildkameras können PINs auf Geldautomaten verraten, www.golem.de 24.08.2015).

Mikroben identifizieren Personen und Umgebungen

Die Bakterien eines Menschen sind fast so charakteristisch wie ein Fingerabdruck. Auch Rückschlüsse auf den Aufenthaltsort sind möglich. Mehr als 1.000 Mikrobenarten siedeln auf und vor allem im Körper des Ökosystems Mensch. Die meisten von ihnen sind passiv und machen keinen Ärger. Viele nützen dem Menschen, indem sie Nahrungsmittel in verwertbare Substanzen verwandeln, Krankheitserreger fernhalten oder das Immunsystem trainieren. Nur die wenigsten verursachen unter Umständen Krankheiten. Bei jedem Menschen sieht diese Mischung ein kleines bisschen anders aus. Die mikrobielle Bevölkerung ist so individuell zusammengewürfelt, dass sie sich eignet, um ihren jeweiligen menschlichen Gastgeber eindeutig zu identifizieren - etwa wie ein Fingerabdruck oder eine Analyse des Erbguts.

Forschende um den Biostatistiker Curtis Huttenhower von der Harvard School für Öffentliche Gesundheit haben in einem Beitrag im Fachjournal „PNAS“ beschrieben, wie das praktisch funktionieren kann, welche Schwierigkeiten damit verbunden sind und welche ethischen Probleme das aufwirft. Sie haben einen Computeralgorithmus entwickelt, der Bakterienproben von Freiwilligen ihren SpenderInnen zuordnen soll. An 120 Versuchsteilnehmenden erprobte die Forschungsgruppe ihre Software und kam zu sehr gemischten Ergebnissen, abhängig davon, von welcher Körperstelle die Bakterienproben genommen worden waren. Auf der Haut veränderte sich die mikrobielle Zusammensetzung bei den meisten ProbandInnen im Laufe der Zeit so sehr, dass nur 30 von 100 Proben eindeutig zugeordnet werden konnten. Bei Stuhlproben hingegen lag die Quote deutlich höher. Ein Jahr nach der ersten Analyse konnten die Forschenden in acht von zehn Fällen frische Stuhlproben richtig der Spendeperson zuweisen.

Die Bakterien könnten der Forensik verraten, ob ein Verdächtiger am Tatort war. Um etwa Einbrecher anhand ihrer hinterlassenen Mikroben zu identifizieren, scheint diese Methode jedoch wesentlich schlechter geeignet zu sein als die Gen-Untersuchung biologischer Proben oder der klassische Fingerabdruck. Der Grund dafür dürfte die Veränderlichkeit des Mikrobioms sein, also die Gesamtheit aller mikrobiellen Mitbewohner des Menschen, von Tieren oder auch Pflanzen. Abhängig davon, was man isst, wem man die Hand geschüttelt hat oder wohin man verreist, verändert sich die Zusammensetzung der mikroskopischen Untermieter fortwährend. Die Untersuchung Huttenhowers hat gezeigt, dass die Lebensgemeinschaft im Darm am stabilsten ist. Selbst nach einer Behandlung mit für Bakterien tödlichen Antibiotika stellt sich bei den meisten Menschen

nach wenigen Wochen wieder größtenteils die Bevölkerung ein, die schon vor der Behandlung im Verdauungstrakt gesiedelt hat. Erst mehrere Antibiotikakuren bringen das Mikrobiom mitunter so durcheinander, dass es sich nicht mehr richtig erholt. Auch die Ernährung hat einen starken Einfluss auf das Mikrobiom. Bei Vegetariern dominieren andere Bakterienarten als bei Fleischessern. Nach ein paar Tagen Fleischverzicht gleicht ihre Bakterienmischung allerdings der von Vegetariern.

Auch jede andere Interaktion mit der Umwelt hinterlässt Spuren im Mikrobiom. Der Heidelberger Biochemiker Peer Bork konnte zeigen, dass sich anhand des Mikrobioms bestimmen lässt, woher ein Mensch stammt. Sogar kurze Aufenthalte in einer anderen Stadt hinterlassen Spuren in der Bakterienbevölkerung; allerdings verschwinden sie in der Regel auch rasch wieder. Das macht mikrobielle Spuren interessant für ein neues Forschungsgebiet, die bakterielle Forensik. Dazu berichtet eine weitere Forschungsgruppe im Fachblatt „Microbiome", dass man anhand der Bakterien auf der Oberfläche eines Mobiltelefons bestimmen kann, an welchem Ort sich der Besitzer zuletzt aufgehalten hat. Die Gruppe um den Genetiker Simon Lax von der University of Chicago hatte auf drei Fachkongressen Kollegen darum gebeten, Abstriche von deren Handys nehmen zu dürfen. Zurück im Labor konnten Lax und Kollegen recht zuverlässig nachweisen, von welchem Veranstaltungsort die jeweilige Probe stammte. Lax ließ außerdem zwei Probanden jede Stunde einen Abstrich von ihrer Schuhsohle und dem Boden nehmen, auf dem sie gerade zufällig standen. Die Analyse zeigte, dass sich die Bakterienzusammensetzung unter der Sohle zwar sehr schnell von Ort zu Ort verändert, trotzdem ließen sich vorherige Aufenthaltsorte grob bestimmen (Meine Mikroben, deine Mikroben, SZ 12.05.2015, 14).

Churchix erfasst Angesicht von Kichergängern

Das israelisch-amerikanische Unternehmen Face-Six hat eine Software zur Gesichtserkennung namens „Churchix" entwickelt, die in Kirchen eingesetzt wird, um zu registrieren, wer am Gottesdienst teilnimmt und wer schwänzt. Gemäß Firmenchef Moshe Greenshpan verwenden bisher 42 Kirchen weltweit die Software und zwar in den USA, Portugal, Afrika, Indonesien und Indien: „Die Reaktionen sind überwältigend. Die Kirchen, mit denen wir gesprochen haben, sagen, für sie sei ein Traum wahr geworden." Die Gemeinden laden Churchix auf einen gewöhnlichen Rechner. In der Datenbank hinterlegen sie hochauflösende Bilder der Gemeindemitglieder. Entweder in der Kirche oder an einer Kontrollstation am Eingang werden Kameras installiert und mit dem System verbunden. Churchix nimmt in Sekundenschnelle ein Abgleich der aufgenommenen mit den hinterlegten Bildern vor. Die Trefferquote liegt, so Greenshpan, bei 99%.

Zweck des Verfahrens ist die Erfassung der Zahl der Kirchenbesuchenden. Die Geistlichen sollen detaillierte Statistiken und Profile über den Kirchgang ihrer Gottesdienstbesuchenden einschließlich Alter und Geschlecht erstellen können. Eine Sprecherin der Evangelischen Kirche in Deutschland (EKD) sagte: „Der Einsatz einer solchen Software zur Überwachung der Gottesdienstbesucher ist rechtlich bei uns undenkbar." Eine Videoüberwachung – und Churchix gehe ja noch weiter als das – sei nur in engen Grenzen möglich, die im Datenschutzgesetz der EKD festgehalten sind. Die stellv. Sprecherin der Deutschen Bischofskonferenz Daniela Elpers ergänzte: „Eine derartige Videoüberwachung in katholischen Kirchen in Deutschland ist derzeit nicht denkbar und entspricht nicht unserer ´Kirchenkultur`, die sich von der amerikanischen in vielen Aspekten unterscheidet". Face-Six arbeitet ansonsten mit Sicherheitsdiensten zusammen. Zu den Kunden gehören z. B. Casinos, Flughäfen und Einkaufszentren. Die spezielle Entwicklung von Churchix geht auf Anfragen von Kirchen zurück (epd, Gesichtserkennung auf der Kirchenbank, Schleswig-Holstein am Sonntag, 23.08.2015, Online S. 19).

Werbeblocker immer weiter verbreitet

Immer mehr Internetnutzende verwenden sogenannte Werbeblocker. Die Zahl der Nutzenden solcher Angebote stieg innerhalb eines Jahres zum zweiten Quartal 2015 um 41% auf 198 Millionen Nutzer pro Monat. Ein installierter Werbeblocker oder Werbefilter entfernt automatisch Werbung von Websites. Der Nutzende bekommt dann entsprechende Texte, Bilder oder Filme nicht mehr zu sehen. Laut der von den Softwareunternehmen Adobe und Page-Fair erstellten und am 10.08.2015 veröffentlichten Untersuchung „The Cost of Ad Blocking" nutzen in Deutschland bereits 18 Millionen Menschen im Internet einen Werbeblocker. Deutschland verzeichnete einen Anstieg von 17%, die USA sogar um 49% und Großbritannien um 82%. Den Anbieter von Inhalten kostet das der Studie zufolge viel Geld. Allein in diesem Jahr gehen dadurch weltweit 21,8 Milliarden Dollar an Werbeeinnahmen verloren. Für 2016 wird sogar mit Verlusten in Höhe von 41,4 Milliarden Dollar gerechnet. Das Problem verschärft sich, weil immer mehr Menschen Werbeblocker auch auf mobilen Endgeräten benutzen könnten. Bisher liegt deren Anteil nur bei 1,6% (Werbeblocker werden immer beliebter, SZ 11.08.2015, 19).

Jetzt DVD-Mitglied werden:
www.datenschutzverein.de
3456034296D
1234544218D
7890908072D

Rechtsprechung

EuGH

Nationales Datenschutz gilt bei effektiver Niederlassung

Der Europäische Gerichtshof (EuGH) entschied mit Urteil vom 01.10.2015, dass das Datenschutzrecht eines Mitgliedstaates auf eine ausländische Gesellschaft angewendet werden kann, wenn diese in diesem Staat mittels einer festen Einrichtung eine tatsächliche und effektive Tätigkeit ausübt (C-230/14). Dem Urteil liegt folgender Sachverhalt zu Grunde:

Weltimmo, eine in der Slowakei eingetragene Gesellschaft, betreibt eine Website zur Vermittlung von in Ungarn gelegenen Immobilien. In diesem Rahmen verarbeitet sie personenbezogene Daten der InserentInnen. Die Inserate sind einen Monat lang kostenlos, danach muss dafür bezahlt werden. Zahlreiche InserentInnen verlangten per E-Mail die Löschung ihrer Inserate am Ende des ersten Monats und gleichzeitig die Löschung der sie betreffenden personenbezogenen Daten. Weltimmo kam dem aber nicht nach und stellte den Betreffenden eine Rechnung aus. Da die in Rechnung gestellten Beträge nicht bezahlt wurden, übermittelte Weltimmo die personenbezogenen Daten der InserentInnen an verschiedene Inkassounternehmen. Dies führte zu Beschwerden bei der ungarischen Datenschutzbehörde. Diese verhängte gegen Weltimmo ein Bußgeld von 10 Mio. ungarischen Forint (HUF) (etwa 32.000 €) wegen Verletzung des ungarischen Gesetzes, mit dem die Europäische Datenschutzrichtlinie (EG-DSRl) umgesetzt wird. Auf die Anfechtung von Weltimmo gegen diese Entscheidung vor ungarischen Gerichten, machte im Kassationsverfahren der oberste Gerichtshof Ungarns, die Kúria, eine Vorlage beim EuGH.

War der ungarischen Kontrollstelle erlaubt, ungarisches Datenschutzrecht anzuwenden und das dort vorgesehene Bußgeld zu verhängen? Gemäß der EG-DSRl sind die nationalen Datenschutzkontrollstellen dafür zuständig, im Hoheitsgebiet ihres Mitgliedstaats insbesondere Untersuchungs- und Einwirkungsbefugnisse auszuüben, unabhängig von der Frage, welches einzelstaatliche Recht materiellrechtlich auf die jeweilige Verarbeitung anwendbar ist. Zudem kann jede Kontrollstelle von einer Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersucht werden. Mit dem vorliegenden Urteil weist der EuGH darauf hin, dass nach der EG-DSRl jeder Mitgliedstaat die Vorschriften anwenden muss, die er zur Umsetzung dieser Richtlinie erlassen hat, sofern die Datenverarbeitung im Rahmen der in seinem Hoheitsgebiet durch geführten Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche besitzt. Das Vorhandensein eines einzigen Vertreters kann unter bestimmten Umständen ausreichen, um eine Niederlassung zu begründen, wenn dieser mit einem ausreichenden Grad an Beständigkeit für die Erbringung der betreffenden Dienstleistungen im fraglichen Mitgliedstaat tätig ist. Der EuGH stellte klar, dass der Begriff der Niederlassung jede tatsächliche und effektive Tätigkeit, die mittels einer festen Einrichtung ausgeübt wird, umfasst, selbst wenn sie nur geringfügig ist.

Konkret bestätigte der EuGH, dass Weltimmo unstreitig eine tatsächliche und effektive Tätigkeit in Ungarn ausübt. Den Erläuterungen der ungarischen Kontrollstelle zufolge verfügt Weltimmo über einen Vertreter in Ungarn, der im slowakischen Handelsregister unter einer Adresse in Ungarn aufgeführt ist und versucht hat, mit den Inserenten über die Begleichung der unbezahlten Forderungen zu verhandeln. Dieser Vertreter hat den Kontakt zwischen dieser Gesellschaft und den Inserenten hergestellt und die Gesellschaft im Verwaltungsverfahren und vor Gericht vertreten. Weltimmo hat außerdem in Ungarn ein Bankkonto zur Einziehung ihrer Forderungen eröffnet und nutzt dort zur Abwicklung ihrer laufenden Geschäfte ein Postfach. Diese vom vorlegenden Gericht zu prüfenden Umstände weisen nach, dass in Ungarn eine „Niederlassung" im Sinne der Richtlinie besteht mit der Folge, dass die Tätigkeit von Weltimmo dem ungarischen Datenschutzrecht unterliegt. Der EuGH weist darauf hin, dass jede von einem Mitgliedstaat eingeführte Kontrollstelle dafür Sorge zu tragen hat, dass die von allen Mitgliedstaaten zur Umsetzung der EG-DSRl erlassenen Vorschriften im Hoheitsgebiet dieses Mitgliedstaats eingehalten werden. Daher kann sich jede Person zum Schutz der die Person betreffenden Rechte und Freiheiten bei der Verarbeitung personenbezogener Daten an jede Kontrollstelle mit einer Eingabe wenden, selbst wenn das auf diese Verarbeitung anwendbare Recht das eines anderen Mitgliedstaats ist. Im Falle der Anwendung des Rechts eines anderen Mitgliedstaats sind jedoch die Untersuchungsbefugnisse der Kontrollstelle unter Einhaltung insbesondere der territorialen Souveränität der anderen Mitgliedstaaten auszuüben, so dass eine nationale Kontrollstelle keine Sanktionen außerhalb des Hoheitsgebiets ihres Mitgliedstaats verhängen darf. Würde gerichtlich festgestellt, dass Weltimmo in Ungarn nicht über eine „Niederlassung" im Sinne der EG-DSRl verfügt und deshalb das Recht eines anderen Mitgliedstaats gilt, dürfe die ungarische Kontrollstelle folglich nicht die Sanktionsbefugnisse ausüben, die ihr durch das ungarische Recht übertragen worden sind. Gemäß der in der EG-DSRl vorgesehenen Verpflichtung zur Zusammenarbeit obläge es dann dieser Kontrollstelle, die Kontrollstelle des betreffenden anderen Mitgliedstaats zu ersuchen, einen etwaigen Verstoß gegen das Recht dieses Staates festzustellen und die allenfalls in diesem Recht vorgesehenen Sanktionen zu verhängen

(EuGH, PM 01.10.2015, Urteil in der Rechtssache C-230/14 Weltimmo s. r. o. / Nemzeti Adatvédelmi és Információszabadság Hatóság).

BVerfG

Identitätsfeststellung bei Versammlung nur bei konkreter Gefahr

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 24.07.2015 festgestellt, dass die Polizei bei DemonstrationsteilnehmerInnen nur dann eine Identitätsfeststellung vornehmen darf, wenn eine „konkrete Gefahr" für die öffentliche Sicherheit besteht (1 BvR 24.07.2015). Filmt die Polizei eine Versammlung, so darf sie nicht ohne weiteres die Identität von TeilnehmerInnen feststellen, die ihrerseits die PolizistInnen filmen. Sonst bestehe die Gefahr, dass DemonstrantInnen „aus Furcht vor polizeilichen Maßnahmen" auch zulässige Film- und Fotoaufnahmen und damit „Kritik an staatlichem Handeln" unterlassen.

Der Beschwerdeführer war im Januar 2011 auf einer angemeldeten Versammlung, bei der die Polizei Ton- und Bildaufnahmen anfertigte, von der Polizei aufgeforderte worden, sich auszuweisen. Dessen Begleiterin erweckte den Eindruck, sie filme ihrerseits die eingesetzten PolizeibeamtInnen. Der Beschwerdeführer war den Aufforderung auf Aushändigung des Personalausweises nachgekommen und hatte gegen die Maßnahme erfolglos vor dem Verwaltungsgericht und dem Oberverwaltungsgericht geklagt. Das BVerfG stellte fest, dass bei der Anwendung des einfachen Rechts, hier § 13 Abs. 1 Nr. 1 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (NSOG), das Recht auf informationelle Selbstbestimmung berücksichtigt werden muss. Präventivpolizeiliches Einschreiten wegen Lichtbildern und Videoaufnahmen erforderten eine konkrete Gefahr für ein polizeiliches Schutzgut, was nur im Einzelfall festgestellt werden könne. In verfassungskonformer Auslegung der §§ 22, 23 des Kunsturhebergesetzes (KUG) müsse davon ausgegangen werden, dass unzulässige Lichtbilder nicht auch stets verbreitet werden. Meinen Sicherheitsbehörden, dass eine Verbreitung von Bildern unzulässig erfolgt, so bedarf es hierfür hinreichend tragfähiger Anhaltspunkte. Die bloße Möglichkeit einer strafbaren Verletzung des Rechts am eigenen Bild genüge nicht. Im konkreten Fall hätte der Anlass für die Bilderstellung darin liegen können, dass diese eine Reaktion auf die polizeilicherseits gefertigten Bild- und Tonaufnahmen waren, etwa zur Beweissicherung mit Blick auf etwaige Rechtsstreitigkeiten. Es könne nicht unterstellt werden, dass die Aufnahmen unter Verletzung von § 33 Abs. 1 KUG im Internet veröffentlicht werden (BVerfG, PE v. 08.10.2015, Identitätsfeststellung im Rahmen einer Versammlung erfordert konkrete Gefahr für polizeiliches Schutzgut).

BVerfG

Vorläufig keine Löschung von Zensus 2011-Daten

In einem Normenkontrollverfahren auf Antrag des Berliner Senats hat der Zweite Senat des Bundesverfassungsgerichts (BVerfG) mit Beschluss vom 26.08.2015 die Löschung der im Rahmen des Zensus 2011 erhobenen Daten per einstweilige Anordnung vorläufig gestoppt (Az. 2 BvF 1/15). § 19 des Zensusgesetzes 2011 wird bis zur Entscheidung in der Hauptsache, längstens für sechs Monate außer Vollzug gesetzt. Das BVerfG nahm eine Folgenabwägung vor: Die längere Datenspeicherung vertieft zwar – geringfügig – den Eingriff in das Recht der betroffenen Bürgerinnen und Bürger auf informationelle Selbstbestimmung. Demgegenüber wiegen die Vorteile, die die einstweilige Anordnung für die Rechtsschutzmöglichkeiten der Gemeinden mit sich bringt, schwerer. Die Löschung der Daten könnte den Gemeinden die Möglichkeit nehmen, eine etwaige fehlerhafte Berechnung ihrer Einwohnerzahl gerichtlich effektiv überprüfen und gegebenenfalls korrigieren zu lassen.

Der Berliner Senat begehrt in einem Verfahren der abstrakten Normenkontrolle, § 7 Abs. 1 und Abs. 2 und § 19 des Zensusgesetzes 2011 sowie § 2 Abs. 2 und Abs. 3 der Stichprobenverordnung und § 19 des Zensusgesetzes 2011 für nichtig zu erklären. Nach dem Zensusgesetz 2011 führten die statistischen Ämter des Bundes und der Länder eine Bevölkerungs-, Gebäude- und Wohnungszählung zum 09.05.2011 durch, um die Einwohnerzahlen von Bund, Ländern und Gemeinden verbindlich festzustellen. Das Amt für Statistik Berlin-Brandenburg stellte für das Land Berlin eine Einwohnerzahl von 3.292.365 Personen fest; dies sind ca. 180.000 Personen weniger als nach den fortgeschriebenen Zahlen auf Grundlage der Volkszählungen von 1981 (Ost) und 1987 (West). Insgesamt haben mehr als 1.000 Gemeinden ebenso wie Berlin gegen die ihre Einwohnerzahlen feststellenden Bescheide Rechtsbehelfe eingelegt.

In dem einstweiligen Verfahren wog – nach einem strengen, restriktiven Maßstab – das BVerfG die Nachteile ab, die einträten, wenn keine Anordnung erginge, der Antrag aber in der Hauptsache Erfolg hätte, gegenüber den Nachteilen, die entstünden, wenn die begehrte einstweilige Anordnung erlassen würde, dem Antrag in der Hauptsache aber der Erfolg zu versagen wäre. Es stellte fest, dass der Ausgang des Normenkontrollverfahrens offen ist. Zur Abwehr möglicher schwerer Nachteile für die betroffenen Gemeinden sei der Erlass der einstweiligen Anordnung dringend geboten. Erginge die einstweilige Anordnung nicht, erwiese sich § 19 des Zensusgesetzes 2011 aber später als verfassungswidrig, so wären die im Rahmen des Zensus 2011 erhobenen Daten, sofern nicht schon geschehen, grundsätzlich unverzüglich zu löschen. Die im Gesetz vorgesehene Frist für die maximale Aufbewahrung dieses Datenmaterials ist am 09.05.2015 abgelaufen. Soweit die Löschung auch Datenmaterial zu Gemeinden betrifft, deren Rechtsschutzverfahren noch nicht rechtskräftig abgeschlossen sind, wäre eine Überprüfung der Rechtmäßigkeit der festgestellten Einwohnerzahl erheblich erschwert, wenn nicht gar unmöglich. Methodik und Qualität der Durchführung der Zensuserhebung könnten einer rechtlichen Würdigung jedenfalls nicht mehr anhand der umstrittenen Daten und Unterlagen - ge-

gebenenfalls unter Hinzuziehung von Sachverständigen - unterzogen werden.

Erginge die einstweilige Anordnung und erwiese sich § 19 des Zensusgesetzes 2011 im Hauptsacheverfahren als verfassungsgemäß, so könnte den klagenden Gemeinden in den noch laufenden Rechtsschutzverfahren eine gerichtliche Überprüfung der festgestellten Einwohnerzahlen ermöglicht werden. Dies wäre zwar mit einem Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger verbunden, der nachträglich nicht mehr rückgängig gemacht werden könnte. Würde im Hauptsacheverfahren letztlich die Verfassungsgemäßheit des § 19 Zensusgesetz 2011 festgestellt, so wiege der davor erfolgte Grundrechtseingriff nicht besonders schwer, da die Speicherung der erhobenen Daten lediglich für einen begrenzten Zeitraum fortdauern würde.

Die von den Statistikämtern festgestellten Einwohnerzahlen des Zensus 2011 sind für den Zeitraum bis zur nächsten Erhebung im Jahre 2021 Grundlage der jeweiligen Zuweisungen der Länder und des Länderfinanzausgleichs nach Art. 107 GG. Sollten die Zahlen tatsächlich unzutreffend sein, könnten darauf beruhende Zahlungen zwar grundsätzlich rückabgewickelt werden. Diese Möglichkeit wäre jedoch ausgeschlossen, wenn die Unrichtigkeit der Zahlen nicht mehr festgestellt werden könnte, weil das zugrunde liegende Datenmaterial vor einer gerichtlichen Sachverhaltsfeststellung gelöscht und entsprechende Unterlagen vernichtet worden wären. Allein für das antragstellende Land Berlin bedeutet die Korrektur seiner Einwohnerzahl um ca. 180.000 nach unten nach seinen Angaben eine Verringerung von Zuteilungen aus dem Länderfinanzausgleich um ca. 470 Millionen Euro pro Jahr, das heißt 4,7 Milliarden Euro für den Zeitraum 2011 bis 2021. Auch für andere große Städte führt der Zensus zu großen Etatlücken, etwa Aachen 10 Mio. Verlust, Bonn 12 Mio. oder Stuttgart 13 Mio. Euro. Darüber hinaus knüpfen z. B. die Rechtsvorschriften über die Einteilung der Bundestagswahlkreise oder die Anzahl der Stimmen im Bundesrat an die Einwohnerzahlen an (BVerfG PE Nr. 63/2015 v. 01.09.2015).

BVerwG

Keine Anspruch der Presse auf Selektorenliste

Das Bundesverwaltungsgericht (BVerwG) hat mit Beschluss vom 20.07.2015 entschieden, dass die Presse keinen Anspruch darauf haben, dass der Bundesnachrichtendienst (BND) ihr Auskunft zum Inhalt der Selektorenliste der National Security Agency (NSA) der USA erteilt (Az. 6 VR 1.15).

Der Redaktionsleiter einer Zeitung, der Antragstellerin, bat den BND um Auskunft darüber, welche Unternehmen mit Sitz in Deutschland und welche deutschen Staatsangehörigen auf der Selektorenliste der NSA gestanden hätten, die dem BND überreicht worden sei, welche Unternehmen mit Sitz in Deutschland und welche deutschen Staatsangehörigen der Bundesnachrichtendienst von der ihm überreichten Selektorenliste der NSA gestrichen habe, welche Unternehmen mit Sitz in Deutschland und welche deutschen Staatsangehörigen der Bundesnachrichtendienst auf der ihm überreichten Selektorenliste der NSA belassen und abgehört habe. Der BND lehnte die Beantwortung dieser Fragen ab. Er äußere sich zu operativen Aspekten seiner Arbeit nur gegenüber der Bundesregierung und den geheim tagenden Gremien des Deutschen Bundestages. Die Antragstellerin beantragte daraufhin beim BVerwG, die Antragsgegnerin durch einstweilige Anordnung zu verpflichten, die erbetene Auskunft zu erteilen.

Dies wurde vom BVerwG abgelehnt. Das Grundrecht der Pressefreiheit begründe keinen Anspruch auf die begehrte Auskunft. Dieses Grundrecht verleiht der Presse zwar einen verfassungsunmittelbaren Anspruch auf Auskunft gegenüber Bundesbehörden, soweit auf sie die Landespressegesetze wegen einer entgegenstehenden Gesetzgebungskompetenz des Bundes nicht anwendbar sind, wie dies u. a. für den BND zutrifft. Der begehrten Auskunft stünden aber berechtigte schutzwürdige Interessen des BND an der Vertraulichkeit der streitigen Selektorenliste entgegen. Für operative Vorgänge im Bereich des BND, nämlich die Beschaffung und Auswertung von Informationen von außen- und sicherheitspolitischer Bedeutung, seien Auskünfte an die Presse generell ausgeschlossen, ohne dass es insoweit einer einzelfallbezogenen Abwägung mit gegenläufigen Informationsinteressen der Presse bedürfte. Der BND habe die ihm gesetzlich zugewiesene Aufgabe, zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen zu sammeln und auszuwerten. Derartige Informationen dürfe der BND nach der für ihn geltenden gesetzlichen Grundlage heimlich unter anderem mit nachrichtendienstlichen Mitteln beschaffen und müsse dies in vielen Fällen tun. Um die ihm gesetzlich zugewiesenen Aufgaben erfüllen zu können, sei der BND mithin darauf angewiesen, verdeckt zu arbeiten. Müssten Auskünfte über solche Vorgänge erteilt werden, würde die Gewinnung von weiteren Informationen erschwert, wenn nicht verhindert, und wäre damit die Erfüllung der Aufgaben des BND gefährdet. Zu den operativen Vorgängen im Bereich des BND gehörten das Ob sowie Art und Umfang der Zusammenarbeit mit ausländischen Nachrichtendiensten. Um außen- und sicherheitspolitisch relevante Erkenntnisse zu gewinnen, sei der BND in vielen Fällen auf die Zusammenarbeit mit ausländischen Nachrichtendiensten angewiesen, indem in gemeinsamem Zusammenwirken Informationen von beiderseitigem Interesse beschafft werden oder anderweitig gewonnene Erkenntnisse ausgetauscht werden. Dabei erfährt der BND beispielsweise, welches Erkenntnisinteresse der ausländische Nachrichtendienst verfolgt. Die Zusammenarbeit setze voraus, dass die beteiligten Nachrichtendienste sich wechselseitig darauf verlassen können, dass von ihnen für geheimhaltungsbedürftig angesehene Informationen auch von der anderen Seite geheim gehalten werden. Die künftige Erfüllung der Aufgaben des BND könne mithin dadurch beeinträchtigt werden, dass im Falle einer Offenlegung von Informationen die Zusammenarbeit mit Nachrichtendiensten anderer Staaten und damit die künftige eigene Gewinnung von außen- und sicherheitspolitischen Erkenntnissen erschwert würde. Dazu käme es, wenn die

Antragsgegnerin Informationen unter Missachtung einer zugesagten oder vorausgesetzten Vertraulichkeit gleichwohl an Dritte bekannt gibt (http://www.bverwg.de/entscheidungen/entscheidung.php?ent=200715B6VR1.15.0).

VG Stuttgart

Verdachtsunabhängige Grenzkontrollen unzulässig

Die Bundespolizei darf gemäß einem Urteil des Verwaltungsgerichts (VG) Stuttgart im Grenzgebiet nicht verdachtsunabhängig Personen kontrollieren, um illegal Einreisende aufzuspüren (Az. 1 K 5060/13). Die Regelung in § 23 Bundespolizeigesetz (BPolG), die ihr im 30 km-Grenzgebiet jederzeit anlasslose Identitätsfeststellungen erlaubt, ist danach europarechtswidrig und deshalb nicht anwendbar. Geklagt hatte ein dunkelhäutiger Mann, der 2013 in einem ICE im deutschen Grenzgebiet zu Frankreich ohne Anlass kontrolliert wurde und sich in seinem Recht auf informationelle Selbstbestimmung verletzt fühlte. Das Gericht ließ offen, ob die Kontrolle verhältnismäßig war und ob generell gezielte Kontrollen „ausländisch" aussehender Menschen diskriminierend sind („racial profiling"). Das VG hielt schon die Ermächtigungsnorm § 23 Abs. 1 Nr. 3 BPolG für rechtswidrig, weil sie gegen den Schengener Grenzkodex verstoße. Diese im Jahre 2006 erlassene EU-Verordnung (Nr. 562/2006) verfolgt das Ziel, die Politiken zur Kontrolle der Außen- und Binnengrenzen innerhalb des Schengen-Raumes zu regeln.

Das VG Stuttgart vertrat die Ansicht, dass der Schengener Grenzkodex verdachtsunabhängige Personenkontrollen im Grenzgebiet zu anderen Schengen-Staaten verbietet, soweit solche Maßnahmen die gleiche Wirkung wie Grenzkontrollen haben. Anlasslose Personenkontrollen könnten nur zulässig sein, wenn diese tatsächlich nicht die Kontrolle der Grenze bezwecken und sich äußerlich auch eindeutig von systematischen Personenkontrollen an den Außengrenzen unterscheiden, d. h. insbesondere nur stichprobenartig durchgeführt werden. Kein Problem hatte das Gericht mit Kontrollen, die aufgrund konkreter Informationen oder Erfahrungen in Bezug auf mögliche Bedrohungen der öffentlichen Sicherheit angeordnet werden, insbesondere zur Bekämpfung der grenzüberschreitenden Kriminalität.

Das Gericht stützte sich auf eine Entscheidung des EuGH, der mit Urteil vom 22.06.2010 in einem französischen Fall diese Linie vorgegeben hatte (C-188/10 u. C-189/10, Melki und Abdeli): Die Ermächtigungsnorm lenke das Handeln der Behörden nicht ausreichend. Um zu verhindern, dass Personenkontrollen die gleiche Wirkung wie Grenzkontrollen entwickeln, verlangte der EuGH, dass den nationalen Polizeigesetzen verbindliche Anhaltspunkte über die Häufigkeit und Intensität der Kontrollen zu entnehmen sind, was in §23 Abs. 1 Nr. 3 BPolG nicht der Fall ist. Aus diesem Grund läuft momentan ein Vertragsverletzungsverfahren der Europäischen Kommission gegen die Bundesrepublik Deutschland (vgl. BT-Drs. 18/4149), dessen Ergebnis aussteht.

Der kurz vor der Entscheidung des VG gefällte Entschluss der Bundesregierung, die Kontrollen an den deutschen Binnengrenzen des Schengen-Raums vorübergehend wieder einzuführen, wird durch das Urteil nicht berührt. In diesem Ausnahmefall ist es der deutschen Bundespolizei auf Grundlage des § 23 Abs. 1 Nr. 3 BPolG gestattet, auch im 30 km-Grenzbereich Personenkontrollen durchzuführen, die faktisch wie Grenzkontrollen wirken (Müller, VG Stuttgart: Europarecht bremst Grenzschützer, http://www.verfassungsblog.de 24.10.2015; Unzulässige Kontrollen, SZ 24./25.10.2015, 8).

OLG Celle

BILD-Zeitung von Islamisten-Prozess ausgeschlossen

Die BILD-Zeitung wurde vom Oberlandesgericht (OLG) Celle im dortigen Prozess gegen zwei nach Deutschland vom „Islamischen Staat" zurückgekehrte Jugendliche ausgeschlossen. Am 03.08.2015 erhielten die Vertreter der Zeitung die Mitteilung: "Nachdem Sie gegen die mit der Akkreditierung verbundene Absprache, Fotos der Angeklagten nur verpixelt zu veröffentlichen, verstoßen haben, hat der Vorsitzende in Ausübung des ihm übertragenen Hausrechts entschieden, dass die Akkreditierung für Ihr Medium verloren geht." Grund: Die Zeitung hatte den angeklagten mutmaßlichen IS-Terroristen Ebrahim H. gezeigt. Auf die Beschwerde der Zeitung hin bestätigte das Gericht am 06.08.2015 seine Entscheidung. Diese sorgte in der Medienwelt wie auch beim Deutschen Journalisten Verband (DJV) für Irritation, weil Ebrahim H. sich vorher ausführlich in einem NDR-Interview geäußert und dabei offen gezeigt und zudem der Süddeutschen Zeitung ein Interview gegeben hatte. Ein Verlags-Syndikus kündigte an, man wolle die Sache nun dem BGH vorlegen (Niederlage für die „Bild", SZ 07.08.2015, 25; „BILD" vom „IS-Prozess" am OLG ausgeschlossen, celleheute.de 03.08.2015).

LG Osnabrück

Bewährungsstrafe für Patientinnen filmenden Arzt

Ein 62-jähriger Hausarzt wurde am 16.09.2015 vom Landgericht (LG) Osnabrück zu zwei Jahren Haft, ausgesetzt zur Bewährung, verurteilt, weil dieser bei Untersuchungen mit einer Kugelschreiberkamera heimlich intime Aufnahmen von Patientinnen gemacht und sie teilweise sexuell missbraucht hatte. Darüber hinaus hatte er kinder- und jugendpornografische Bilder und Fotos besessen. Neben der Bewährungsstrafe verhängte das Gericht zudem ein dreijähriges Berufsverbot und eine Geldauflage von 75.000 Euro. Das Geld muss er laut Richterspruch an gemeinnützige Organisationen zahlen.

Der Vorsitzende Richter Dieter Temming erklärte, dass der Angeklagte trotz des zeitlich begrenzten Berufsverbots nie wieder als Arzt arbeiten werde, da dieser zugesagt habe, seine Approbation zurückzugeben. Deshalb bestehe auch keine Wiederholungsgefahr: „Der Angeklagte steht vor den Trümmern seiner privaten und beruflichen Existenz." Dies sei ein Grund für eine Bewährungsstrafe gewesen. Zudem habe das Geständnis des Angeklagten für ihn gesprochen und

die Tatsache, dass er seinen Opfern bereits ein hohes Schmerzensgeld gezahlt habe. Auch Verteidiger und Staatsanwaltschaft hatten sich in ihren Plädoyers für eine zur Bewährung ausgesetzte Haftstrafe ausgesprochen.

Das Gericht verurteilte den Mediziner für 70 Fälle, in denen er seine Patientinnen gefilmt hatte. In zwölf Fällen habe er die Frauen zudem sexuell motiviert etwa an den Brüsten berührt, ohne dass dies für eine Untersuchung notwendig gewesen sei. Die Opfer seien in diesen Fällen Frauen gewesen, die körperlich beziehungsweise geistig behindert waren. Der Angeklagte hatte sich im Prozess an seine früheren Patientinnen gewandt und für seine Taten entschuldigt: „Ich weiß nicht, was mich getrieben hat." Zu Prozessbeginn hatte der Arzt ein Geständnis abgelegt. Die zahlreichen Journalisten und Zuschauenden hatten den Gerichtssaal vor der Aussage des Angeklagten verlassen müssen. Die Vorwürfe gegen den Mann waren im November 2013 bekannt geworden. Die Filmaufnahmen der Patientinnen hatten die Ermittler durch Zufall entdeckt. Sie durchsuchten die Wohnung des Arztes - und fanden neben 80.000 Bildern und Videoaufnahmen von Kindern und Jugendlichen in eindeutigen Posen auch die Filme von den Patientinnen. Der Arzt hatte die Bilder und Videos auf einem Downloadportal angeboten und getauscht (Osnabrücker Arzt zu Bewährungsstrafe verurteilt, www.ndr.de 16.09.2015).

VG Schleswig

VSA scheitert gegen ULD mit Äußerungsverbot

Mit rechtskräftigem Beschluss vom 25.08.2015 wies das Verwaltungsgericht (VG) Schleswig den Antrag des bayerischen Apothekenrechenzentrums VSA GmbH zurück, gegen das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) ein Ordnungsgeld zu verhängen für Äußerungen des damaligen ULD-Leiters Thilo Weichert in der Zeitschrift „Datenschutz und Datensicherheit" - DuD (Az. 8 D 3/15). Das Verfahren ist eines in einer Reihe von mehreren Prozessen, mit denen die VSA das ULD überzogen hat.

Hintergrund ist der Verkauf von angeblich anonymisierten Rezeptdaten u. a. an die Pharmaindustrie durch die VSA. Das ULD hatte diese kommerzielle Verwertung öffentlich als gewaltigen Datenschutzskandal bewertet. Die zuständige Aufsichtsbehörde, das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) erließ deshalb für den Zeitraum bis 2010 zwei Bußgeldbescheide gegen die VSA und den Dienstleister pharmafact in Höhe von 40.000 und 110.000 €. In Bezug auf die Praxis der VSA behauptet das BayLDA jedoch, dass durch eine Umstellung des Verfahrens nun eine wirksame Anonymisierung vor dem Verkauf der Rezeptdaten erfolge. Dies wurde jedoch im Düsseldorfer Kreis von einigen anderen Aufsichtsbehörden anders bewertet, u. a. vom ULD. Dessen Leiter Thilo Weichert äußerste sich entsprechend auf Presseanfragen hin öffentlich. Dies veranlasste die VSA dazu, vor dem VG Schleswig gegenüber dem ULD am 05.11.2013 eine Untersagungsverfügung zu bewirken (abgedruckt unter ZD 2014, 102). Nachdem eine entsprechende Meldung des virtuellen Datenschutzbüros, dessen Geschäftsführung beim ULD liegt, die über den Vorgang berichtete, nicht rechtzeitig gelöscht wurde, erwirkte die VSA beim VG Schleswig mit Beschluss vom 03.12.2013 ein Ordnungsgeld in Höhe von 1.000 € (abgedruckt in ZD 2014, 100). Auf die Beschwerde des ULD hin wurde die Untersagungsverfügung des VG Schleswig mit Beschluss vom 28.02.2014 durch das Oberverwaltungsgericht (OVG) Schleswig-Holstein teilweise wieder aufgehoben bzw. modifiziert (abgedruckt in DuD 2014, 716 mit Anm. Kauß). In dem gerichtlichen Verfahren ging es dem ULD darum, nachzuweisen, dass die VSA auch nach der Verfahrensänderung rechtswidrig pseudonyme Rezeptdaten veräußert. Die Gerichte befassten sich jedoch nicht mit dieser Datenschutzthematik und behandelten ausschließlich die Frage, ob und wie sich das ULD hierzu äußern durfte. Wenig förderlich bei diesem Verfahren war und ist, dass das BayLDA Auskunft über Details den nunmehr praktizierten Umgang der VSA mit den Rezeptdaten selbst gegenüber den anderen Aufsichtsbehörden bis heute verweigert.

Die das Äußerungsrecht von Datenschutzaufsichtsbehörden einschränkenden Entscheidungen des VG Schleswig und des OVG Schleswig-Holstein waren Anlass für eine kritische Auseinandersetzung von Thilo Weichert in der Zeitschrift DuD. Diesen Aufsatz nahm die VSA zum Anlass, das ULD erneut vor den Kadi zu ziehen – diesmal ohne Erfolg.

Im Ergebnis erfolgreich war – mit Unterstützung des BayLDA – die VSA aber bei ihrem Versuch, die bisherige kommerzielle Verwertung der Rezeptdaten fortzuführen und sich dadurch gegenüber anderen Apothekenrechenzentren, die ein valides Anonymisierungsverfahren durchführen, etwa das Norddeutsche Apothekenrechenzentrum (NARZ) in Bremen, einen Wettbewerbsvorteil zu verschaffen. Erfolgreich blieb die VSA weiterhin, ihr praktiziertes Verfahren einer öffentlichen Kontrolle und Kritik zu entziehen.

Zugleich war und ist die VSA insofern erfolgreich, dass sie mit der Vielzahl der Verfahren zu Äußerungen von Datenschutzaufsichtsbehörden ein neues wirksames Drohszenario aufbaute: Das Überziehen mit Prozessen wegen Äußerungen zum Datenschutzrecht bindet viele der nur begrenzt verfügbaren Ressourcen der Aufsichtsbehörden und schreckt sie damit wirksam vor berechtigten Datenschutz-Warnungen ab. Im Folgenden werden die wesentlichen Passagen des aktuellen Beschlusses des VG Schleswig vom 25.08.2015 dokumentiert:

VG Schleswig (Az. 8 D 3/15)

Beschluss in der Vollstreckungssache der VSA GmbH – Vollstreckungsgläubigerin (VG)

Proz.-Bev.: Rechtsanwälte Hogan Lovells International LLP, … Hamburg ...
gegen das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein – Vollstreckungsschuldner (VS)
Proz.-Bev.: Rechtsanwälte Dr. Kauß, … Freiburg im Breisgau ...
Streitgegenstand: Datenschutzrecht – Vollstreckung
hat das Schleswig-Holsteinische Verwaltungsgericht – 8. Kammer – am 25.08.2015 beschlossen:

Der Antrag wird abgelehnt. Die Kosten des Verfahrens trägt die Vollstreckungsgläubigerin (VG).

Die VG – Antragstellerin im Verfahren des einstweiligen Rechtsschutzes – begehrt die Verurteilung des Vollstreckungsschuldners (VS) – Antragsgegner im Verfahren des einstweiligen Rechtsschutzes – zu einem Ordnungsgeld wegen Zuwiderhandlung gegen seine Verpflichtung aus einer einstweiligen Anordnung.

Im einstweiligen Anordnungsverfahren der VG gegen den VS beschloss das Schleswig-Holsteinische Verwaltungsgericht am 05.11.2013 – 8 B 50/13:

„Dem Antragsgegner wird im Wege der einstweiligen Anordnung aufgegeben, es bei Vermeidung eines Ordnungsgeldes von bis zu 250.000 € zu unterlassen, folgende Äußerungen in der Medienöffentlichkeit – insbesondere in der Presse (samt Onlineinhalten), Rundfunk und Fernsehen – sowie im Internet, wörtlich und/oder sinngemäß verbreiten zu lassen:

- die Antragstellerin sei an einem der größten Datenskandale der Nachkriegszeit beteiligt, und/oder
- die Antragstellerin gebe keine anonymisierten, sondern pseudonymisierte Daten heraus, und/oder
- die Antragstellerin handele unzulässig, und/oder
- das Geschäftsmodell der Antragstellerin sei illegal, und/oder
- die von der Antragstellerin vorgenommene Verschlüsselung der Rezeptdaten sei nicht ausreichend, und/oder
- die Antragstellerin begehe einen Rechtsverstoß, und/oder
- die von der Antragstellerin verschlüsselten Datensätze seien eindeutig zuordenbar, und/oder
- eine Zuordnung der Daten zu Patienten sei von der Antragstellerin beabsichtigt, und/oder
- die Antragstellerin handele mit Bereicherungsabsicht.“

Auf Beschwerde des Vollstreckungsschuldners wurde der Beschluss des Schleswig-Holsteinischen Verwaltungsgerichts vom 05.11.2013 – 8 B 50/13 vom Schleswig-Holsteinischen Oberverwaltungsgericht mit Beschluss vom 28.02.2014 – 4 MB 82/13 – wie folgt geändert:

„Der Antrag wird hinsichtlich der beantragten Anordnung einer Unterlassung der Äußerungen,

- die Antragstellerin gebe keine anonymisierten, sondern pseudonymisierte Daten heraus, und/oder
- die Antragstellerin handele unzulässig, und/oder
- die von der Antragstellerin vorgenommene Verschlüsselung der Rezeptdaten sei nicht ausreichend, und/oder
- die Antragstellerin begehe einen Rechtsverstoß, und/oder
- die von der Antragstellerin verschlüsselten Datensätze seien eindeutig zuordenbar,

mit der Maßgabe abgelehnt, dass der Antragsgegner zukünftig entsprechende Äußerungen als seine Auffassung zu kennzeichnen hat. Im Übrigen wird die Beschwerde zurückgewiesen.“ …

Die VG hat am 20.05.2015 die Verurteilung des VS zu einem Ordnungsgeld beantragt. Sie macht geltend, dass der VS durch fünf Äußerungen in dem Aufsatz von Herrn Thilo Weichert, „Das Äußerungsrecht der Datenschutzbehörden (Teil 1)“, Datenschutz und Datensicherheit (DuD) 2015, S. 323 – S. 327 sowie wortgleiche Ausführungen im Tätigkeitsgericht 2015 des ULD SH, S. 12 f gegen die einstweilige Anordnung verstoßen habe. Für die Veröffentlichung in DuD 2015, S. 323 – S. 327 sei auch der VS verantwortlich. Aus dem Aufsatz gehe eindeutig hervor, dass sich Herr Weichert als Leiter und vertretungsberechtigtes Organ des VS äußere. …

Der Antrag hat keinen Erfolg …

Der VS hat der einstweiligen Anordnung jedoch nicht zuwider gehandelt. …

In Bezug auf den Aufsatz von Herrn Thilo Weichert in DuD 2015, S. 323 ff. scheitert eine Zuwiderhandlung des VS nicht bereits daran, dass die dort getätigte Äußerung des Autors Weichert dem VS nicht zuzurechnen sind. Nur eigenes Verschulden des Schuldners, bei juristischen Personen die Schuld der für sie handelnden Personen, rechtfertigt eine Verurteilung nach § 890 ZPO (vgl. BVerfG, B. v. 25.10.1966 – 2 BvR 506/63, Rn. 48 – zit. nach juris). Für die Zurechnung gilt § 31 BGB, wonach es eine in Ausführung der dem Organwalter zustehenden Verrichtungen begangenen Handlung bedarf (vgl. MüKo-Gruber, ZPO, 4. Aufl. 2012, § 890 Rdnr. 22). Das Gesetz will mit dieser Formulierung ausdrücken, dass der Organwalter in amtlicher Eigenschaft und nicht lediglich als Privatperson tätig geworden sein muss (vgl. MüKo-Reuter, BGB, 6. Aufl. 2012, § 31 Rdnr. 33). Zwischen Amtstätigkeit und Schädigung muss ein enger, objektiver Zusammenhang bestehen (vgl. BGH, U. v. 30.10.1967 – VII ZR 82/65, NJW 1968, S. 391, 392; das BVerfG, U. v. 16.12.2014 – 2 BvE 2/14, NVwZ 2015, S. 209 stellt für die Frage, wann ein Mitglied der Bundesregierung im politischen Meinungskampf dem Neutralitätsgebot unterworfen ist, darauf ab, ob das Regierungsmitglied für sein Handeln die Autorität des Amtes und die damit verbundenen Ressourcen in spezifischer Weise in Anspruch nimmt).

Herr Thilo Weichert hat nach Überzeugung der Kammer die Ausführungen in DuD 2015, S. 323 ff. in amtlicher Eigenschaft und nicht lediglich als Privatperson getätigt. Er wird in dem Beitrag unter Nennung seiner Amtsbezeichnung und seiner amtlichen Mailadresse bildlich dargestellt. Herr Weichert nimmt in dem Beitrag zudem mehrfach ausdrücklich auf sein Amt Bezug, und zwar zunächst unter Gliederungspunkt 1., wo es heißt: „Diese gegen den Autor als Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und damit der der Datenschutzbehörde des Landes ergangene Entscheidungen sind symptomatisch für ein reduziertes rechtliches Verständnis der Funktion der Aufsichtsbehörden.“ Unter Gliederungspunkt 2. heißt es weiter: „Dies veranlasste den Spiegel im August 2013, erneut zu berichten und den Leiter des ULD damit zu zitieren, …“ Die weiteren Formulierungen unter Gliederungspunkt 2. lassen ebenfalls erkennen, dass dort nicht die persönliche Meinung des Herrn Thilo Weichert, sondern die Auffassung des VS („nach Ansicht des ULD“) wiedergegeben werden soll.

Weder in dem Beitrag „Das Äußerungsrecht der Datenschutzbehörden (Teil 1), DuD 2015, S. 323 ff. noch in

seinem Tätigkeitsbericht 2015, S. 12 f verstößt der VS jedoch durch die VG beanstandeten Äußerungen gegen die einstweilige Anordnung.

Die Äußerung, dass „es traurig wäre, wenn die Dienstleister des Vertrauensberufs Apotheker erst durch Gerichtsprozesse zur Vertraulichkeit zu veranlassen wären“ in DuD 2015, S. 324 sowie im Tätigkeitsbericht 2015 des ULD SH, S. 12 stellt keine Zuwiderhandlung dar, da diese Äußerung dem Antragsgegner nicht ausdrücklich untersagt worden ist und sich diese auch nicht sinngemäß unter die zu unterlassenden Äußerungen fassen lässt.

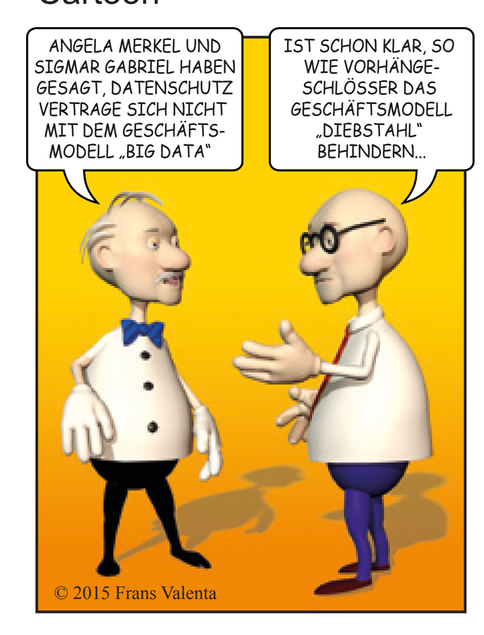
Auch mit der Äußerung, „es handele sich anscheinend um ein ´lohnendes Geschäftsmodell´ durch ´illegale Nutzung der Rezeptdaten´“ in DuD 2015, S. 324 und im Tätigkeitsbericht 2015 des ULD SH, S. 12 verstößt der VS nicht gegen die einstweilige Anordnung. Über den Umfang, was nach dem Ausspruch der einstweiligen Anordnung verboten ist, ist im Verfahren nach § 167 Abs. 1 VwGO i.V.m. § 890 ZPO zu entscheiden (vgl. Zöller/Stöber, ZPO, 28. Aufl. 2010, § 890 Rdnr. 15). Dem bloßen Wortlaut nach ließe sich diese Äußerung sinngemäß zwar unter die zu unterlassende Äußerung „das Geschäftsmodell der Antragstellerin sei illegal“ fassen. Sie fällt aber – im Wege einer restriktiven Auslegung – zum einen deshalb nicht unter diese zu unterlassende Äußerung, weil es sich nicht um eine erneute Meinungskundgabe handelt, sondern eine Äußerung von Herrn Thilo Weichert aus dem Spiegel (August 2013) zitiert wird, was darin zum Ausdruck kommt, dass die Worte „lohnendes Geschäftsmodell“ sowie „illegale Nutzung der Rezeptdaten“ in Anführungszeichen gesetzt werden. Zum anderen ist von Bedeutung, dass diese Äußerung in dem Beitrag deshalb wiedergegeben wird, da diese – neben anderen Äußerungen – Auslöser der Auseinandersetzung zwischen den Beteiligten im Jahr 2013/2014 war, welche schließlich zu den Entscheidungen des Schleswig-Holsteinischen Verwaltungsgerichts vom 05.11.2013 – 8 B 50/13 – sowie des Schleswig-Holsteinischen Oberverwaltungsgerichts vom 28.02.2014 – 4 MB 82/13 – geführt hat. Letztere werden auf S. 324 des Beitrages einer kritischen Betrachtung unterzogen. Diese kritische Betrachtung, welche dem VS in einer freiheitlich demokratischen Grundordnung gestattet sein muss, würde ins Leere laufen, wenn ihm untersagt wäre, den eigentlichen Auslöser der gerichtlichen Verfahren darzustellen.

Die Äußerung, „es bestätigte, dass das ULD die nach seiner Ansicht rechtswidrige Praxis der Datenverarbeitung von Abrechnungszentren unter namentlicher Nennung als illegal und rechtswidrig bezeichnen dürfe“ in DuD 2015, S. 324 sowie die – nahezu wortgleiche – Äußerung „Ausdrücklich bestätigte das OVG, dass das ULD die nach seiner Ansicht rechtswidrige Praxis der Datenverarbeitung von Abrechnungszentren auch weiterhin als illegal und rechtswidrig bezeichnen dürfe, und dies sogar unter namentlicher Nennung“ stellen keine Zuwiderhandlungen gegen die einstweilige Anordnung dar. Die Verwendung des Wortes „illegal“ ist dem VS ebenso wenig untersagt wie der Gebrauch des Wortes „rechtswidrig“. Der VS darf behaupten, dass die VG einen Rechtsverstoß begehe, umgangssprachlich also illegal handele, wenn er dies – wie vorliegend geschehen – als eigene Auffassung kennzeichnet.

Mit den Äußerungen „dieser – nach Ansicht des ULD – sich täglich fortsetzende ´zigmillionenfache Datenschutzverstoß schädigt – nach Ansicht des ULD -“ in DuD 2015, S. 324 und „dieser sich täglich fortsetzende ´zigmillionenfache Datenschutzverstoß schädigt – nach Ansicht des ULD –“ im Tätigkeitsbericht 2015 des ULD SH, S. 13 verstößt der VS ebenfalls nichts gegen die einstweilige Anordnung. Die Äußerungen entsprechen sinngemäß nicht den zu unterlassenden Äußerungen „das Geschäftsmodell der Antragstellerin sei illegal“ und „die Antragstellerin sei an einem der größten Datenskandale der Nachkriegszeit beteiligt“. Die Äußerungen lassen sich, da Datenschutzschutzverstöße beanstandet werden, sinngemäß der Äußerung „die Antragstellerin begehe einen Rechtsverstoß“ zuordnen. Diese Äußerung ist dem VS gestattet, sofern er – wie vorliegend geschehen – diese als eigene Auffassung kennzeichnet.

Mit der Äußerung, „damit war es nicht nur gerichtlich erfolgreich, sondern hat sich damit – auf dem Markt der Apothekenrechenzentren – einen Marktvorteil gegenüber Wettbewerbern gesichert, die rechtskonform agieren“ in DuD 2015, S. 324 – der Tätigkeitsbericht 2015 des ULD SH enthält diese Äußerung nicht –, verstößt der Vollstreckungsschuldner auch nicht gegen die einstweilige Anordnung. Aus der Verwendung des Wortes „rechtskonform“ in Verbindung mit Wettbewerbern der VG ergibt sich zwar im Umkehrschluss, dass die VG nicht rechtskonform, mithin rechtswidrig agiere. Die Äußerung lässt sich daher sinngemäß der Äußerung „die Antragstellerin begehe einen Rechtsverstoß“ zuordnen. Diese Äußerung ist dem VS gestattet, sofern er sie als eigene Auffassung kennzeichnet. Vor dem Wort „rechtskonform“ fehlt zwar der Zusatz „nach Ansicht des ULD“. Aus dem Zusammenhang wird jedoch hinreichend deutlich, dass es sich bei der geäußerten Kritik an der Übermittlungspraxis von Rezeptdaten um die eigene Auffassung des VS handelt („vom ULD als unzulässig bewertete“ im ersten Satz des Absatzes; im zweiten Satz findet sich zweifach der Zusatz „– nach Ansicht des ULD –“; im dritten Satz des Absatzes heißt es „Dass das ULD mit seiner Kritik“; im vierten Satz wird auf die „öffentlich geäußerte Kritik einer Datenschutzbehörde, hier des ULD,“ hingewiesen). Weiterhin lässt sich die beanstandete Äußerung nicht sinngemäß der zu unterlassenden Äußerung „die Antragstellerin handele mit Bereicherungsabsicht“ zuordnen.

Cartoon



Buchbesprechungen

BDSG-Kommentare

(tw) Die DANA-Redaktion wurde darauf hingewiesen, dass uns in der Buchbesprechung des Werkes von Gola/Schomerus in der DANA 2/2015 (S. 104 f.) ein inhaltlicher Fehler unterlaufen ist. Anders als dargestellt, ist der Gola/Schomerus nicht der älteste und einzige BDSG-Kommentar, bei dem eine personelle Kontinuität bis zum heutigen Tag gewahrt worden ist. Ursprünglich hieß der Kommentar Ordemann/Schomerus und Prof. Peter Gola ist erst später eingestiegen. Der Kommentar ist auch nicht der älteste. Die Aussagen zu Alter und Kontinuität treffen vielmehr noch mehr auf die als Loseblattkommentare herausgegebenen und seit 1977 bzw. 1978 erscheinenden Schaffland/Wiltfang und Bergmann/Möhrle/Herb zu. Der Rezensent bittet um Entschuldigung für diesen Fehler.



Bergmann, Lutz/Möhrle, Roland/Herb, Armin,
Datenschutzrecht
Kommentar Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und Kirchen, Bereichsspezifischer Datenschutz
Richard Boorberg, Stand Juli 2015, 49. Ergänzungslieferung, Loseblatt, 3 Bände, ISBN 978-3-415-00616-4

(tw) Für Rezensenten sind Loseblattsammlungen in vieler Hinsicht ein Problem: Rezensionen erlauben immer nur eine Momentaufnahme von einem Werk, das sich möglicherweise noch ändert, das nicht vollständig aktuell sein kann und das durch das Einsortieren der Ergänzungslieferungen einen hohen Pflegeaufwand verursacht. Dessen ungeachtet lohnen sich Besprechungen von solchen Werken erst recht, wenn sie ein Format erreicht haben, das über das gebundener Werke hinausgeht. Diese Aussage trifft für den Bergmann/Möhrle/Herb (BMH) zu, der mit seinem erstmaligen Erscheinen im Jahr 1977 eine fast einzigartige Tradition bei den Datenschutzkommentaren und zugleich eine erstaunliche Aktualität vorweisen kann. Eine Darstellung lohnt auch, wenn der Erwerb des Werks Nutzen verspricht. Letzteres gilt für der BMH insbesondere für den Datenschutzpraktiker, der mit den unterschiedlichsten Datenschutzfragen konfrontiert ist und möglichst alles aus einer Hand haben möchte. Der BMH ist von seiner Grundanlage eine Fundgrube, da er nicht nur das BDSG kommentiert, sondern exemplarisch auch ein Landesdatenschutzgesetz (Baden-Württemberg), sämtliche anderen Landesdatenschutzgesetze dokumentiert, zudem ausführlich das Sozialdatenschutzrecht und das Melderecht – einschließlich des neuen Bundesmeldegesetzes – dokumentiert und teilweise erläutert. Ein Teil VI mit der Überschrift „Multimedia und Datenschutz“ ist zwar bzgl. der Vorschriften weitgehend abgedeckt, dagegen, entgegen der gewaltigen praktischen Relevanz, nur sehr spärlich erläutert – wohl aber mit dem sonst eher vernachlässigten Rundfunkstaatsvertrag. Letzteres ist wohl dem Umstand zuzuschreiben, dass Armin Herb seit vielen Jahren erst beim SWF und nun beim Südwestrundfunk (SWR) auch die Funktion des Rundfunkdatenschutzbeauftragten wahrnimmt. Äußerst materialreich sind auch die Darstellungen zu den verschiedenen Wirtschaftsbranchen im § 28 BDSG. Dagegen ist die Bearbeitung zur Internetdatenverarbeitung bei § 29 BDSG nicht ergiebig.

Die Praktikerorientierung kommt auch dadurch zum Ausdruck, dass viel nützliches Material in die Sammlung mit aufgenommen ist. Dazu gehören Tabellen, Übersichten, Kataloge, Prüfschemata und Muster und letztlich ein äußerst inhaltsreiches Stichwortverzeichnis, das aber – das Los der Loseblattsammlung – auf dem Stand 2011/2012 ist. Dies hindert aber nicht die Aktualität der späteren Lieferungen, die selbst schon die Organisationsreform der Dienststelle der BfDI mit umfassen. Die Darstellungen jüngeren Datums spiegeln den jeweiligen Diskussionsstand zum Thema einschließlich Rechtsprechung und aktuelle Literatur gut dar. So greift der BMH etwa – anders als der „Simitis“ – die moderne Diskussion über die Schutzziele des Datenschutzes auf, und er setzt sich kritisch mit aktuellen Themen wie Passenger Name Record oder TK-Vorratsdatenspeicherung auseinander. Dabei vertritt der Kommentar erfeulich fortschrittliche Positionen mit reichhaltigen Hinweisen und Argumenten. Kritisch zu bewerten sind Passagen, in denen es um die Privilegierung von Rundfunkanstalten oder von Rechtsanwälten geht, etwa wenn die Ansicht vertreten wird, § 43a BRAO verdränge die Anwendbarkeit des BDSG.

Während damit die drei Bände des BMH, die im Bücherregal gute 20 Zentimeter füllen, für den Praktiker in vielen Bereichen, insbesondere die öffentliche Verwaltung, die klassische Privatwirtschaft und den Rundfunk, als Quelle schon alleine oft genügen dürften, kann dies für den Forschenden im Bereich des Datenschutzes nicht gelten. Der Kommentar bleibt in der juristischen Erörterung verhaftet, die technisch zwar kompetent, aber nicht ausführlich und nicht tiefergehend ist. Für die wissenschaftliche Auseinandersetzung liefert der Kommentar immer wieder interessante, nicht abgeschriebene Positionen. Auch hier profitieren die Nutzenden von dem Umstand, dass die Autoren seit Jah-

ren an den aktuellen Diskussionen hautnah beteiligt sind. Vollständigkeit kann nicht erwartet und sollte wohl auch nicht geliefert werden.



Drackert, Stefan
Die Risiken der Verarbeitung personenbezogener Daten – Eine Untersuchung zu den Grundlagen des Datenschutzrechts
Schriftenreihe des Max-Planck-Instituts für ausländisches und Internationales Strafrecht
Freiburg, Duncker & Humblot, Berlin, 2014, ISBN 978-3-86113-806-8 u. 978-3-428-14730-4, 338 S.

(tw) Angesichts der umfangreichen Literatur, die es auf dem deutschen Markt zum Datenschutz gibt, ist es schon ein gewagtes Unterfangen, ein Buch allgemein über die Risiken der personenbezogenen Datenverarbeitung zu verfassen. Dies gilt auch und erst recht, wenn der Autor den Anspruch einer wissenschaftlichen Arbeit, hier einer Doktorarbeit, hat. Man sollte meinen, dass zu den „Grundlagen des Datenschutzrechts" schon alles geschrieben wurde. Um so verblüffender ist es, dass ein solches Buch nicht nur geschrieben, sondern auch noch von der Gesellschaft für Datenschutz und Datensicherheit mit ihrem GDD-Wissenschaftspreis 2014 prämiert wurde. Grund genug, sich das Buch genauer anzuschauen.

Ein vertiefter Blick in dieses Werk zeigt, dass zwar zu den Grundlagen des Datenschutzes schon praktisch alles gesagt wurde. Insofern konnte aber bis heute selbst in Deutschland kein Konsens hergestellt werden. Es ist eine Binsenweisheit, dass ein Konsens erst recht in Europa und noch weiter transatlantisch und global aussteht. Vor diesem Hintergrund sollte dieses Buch gelesen werden, auch wenn der Fokus die deutsche gesetzgeberische, judizierende und wissenschaftliche Debatte ist, wohl aber mit Ausflügen in die europäische Rechtsprechung und in die internationale und europäische Normsetzung. Tatsächlich geht der Konsens in Europa über die „Grundlagen" schon sehr weit, doch gibt es da zum einen den Streit Europas mit der herrschenden Meinung in den USA und zum anderen den Versuch einer Minderheit in Europa, dem Datenschutz auch hierzulande ein geringeres Gepräge zu verpassen.

Diese Versuche können politisch wie auch „wissenschaftlich" kurz dadurch auf den Punkt gebracht werden, dass die Privatwirtschaft von den Fesseln des Gesetzesvorbehalts befreit werden soll. Die Firmen wollen sich bei ihrer Verarbeitung personenbezogener Daten von Kunden und Arbeitnehmern nicht immer mit dem Datenschutz herumschlagen müssen. Diese emotionale Belastung der Wirtschaft dürfte sich angesichts des gewaltigen Vollzugsdefizits zwar im Rahmen halten. Doch sind Gerichtsentscheidungen wie aktuell die des EuGH zur Safe Harbor schon geeignet, eine gewisse Verunsicherung zu produzieren. Tatsächlich muss dies die Motivation des Autors gewesen sein, diese Arbeit zu verfassen, auch wenn er dies so nicht explizit formuliert.

Auch wenn er Privatunternehmen hinsichtlich des Datenschutzes keine Sicherheit geben kann, so scheint es ihm zumindest ein wenig zu gelingen, die „herrschende Meinung" zu verunsichern. Diese Promotion ist derzeit wohl das Ausführlichste und Reflektierteste, was es im deutschen Schrifttum zur Abschaffung des datenschutzrechtlichen Verbots mit Erlaubnisvorbehalt gibt. Dabei formuliert der Autor dies – in klarer Erkenntnis der gehärteten Verfassungs- und Grundrechsrechtsprechung – gar nicht als sein vorrangiges Anliegen, sondern allenfalls als eine Anregung. Es wird ein „pragmatischer Vorschlag zur stärkeren Ausrichtung und Ausdifferenzierung der rechtswissenschaftlichen Bemühungen auf konkrete Verarbeitungsfolgen" unterbreitet, der aber „durchaus" eine „kopernikanische Wende" im Datenschutzrecht zu vollziehen möglich machen würde (S. 320). Während Kopernikus sein Wende durch die Beobachtung der Realität erreichte, verbleibt der Autor in seinem wissenschaftlichen Elfenbeinturm und vertritt dabei ein rückwärtsgewandtes Grundrechtsverständnis ohne realistischen Blick für die Gegenwart und Zukunft der Digitalisierung.

Vorneweg – bei aller folgenden Kritik – einige Komplimente an die Arbeit: Sie ist gut und verständlich geschrieben, wenngleich so manche verwendete Terminologie befremdet, etwa, wenn von „Informationspermanenz" (insbes. S. 299 ff.) oder „Informationsemergenz" (S. 304 f.) die Rede ist. Die Verwendung solcher Wortmonster, die wohl mit „Langlebigkeit von Daten" und mit „Analysepotenzial digitaler Datenverarbeitung" übersetzt werden können, ist sicherlich nicht der Popularisierung der letztlich vertretenen Thesen förderlich. Positiv zu bewerten ist die nicht nur fleißige, sondern auch intellektuell redliche Beschreibung und Analyse von unterschiedlichsten internationalen, europäischen und nationalen Datenschutzinstrumenten, von Rechtsprechung und Literaturmeinungen. Hier liegt eine große Stärke: Mit einer überzeugenden Akribie werden Normen, Urteile und wissenschaftliche Beiträge auf ihre Risikoorientierung hin untersucht. Insofern haben die Ausführungen Informationswert, sind aber nicht gerade neu. Alle Topoi finden sich in unserer Datenschutzliteratur und wurden konsistent und umfassend vom Bundesverfassungsgericht entwickelt und ausdifferenziert. Von den obersten europäischen Gerichten (EGMR und EuGH) wurden diese, wenn auch teilweise erst fragmentarisch, rezipiert.

Hinsichtlich der adressierten Risiken untersucht werden von internationalen Privatheits- und Vertraulichkeitsgarantien über das europäische Primär- und Sekundärrecht, die Rechtsprechung des BVerfG bis hin zu Literaturstimmen fast alle relevanten Äußerungen zu den materiellen Schutzzielen des Datenschutzes. Erhellend und dem praxisorientierten Datenschützern nicht ansatzweise präsent dürften insbesondere die informativ präsentierten Schutzkonzeptionen in der Literatur, beginnend mit Walter Schmidt (1974) und Otto Mallmann (1977) über

die Privatrechtsprotagonisten Karl-Heinz Ladeur und Wolfgang Kilian bis hin zu aktuelleren Ansätzen von Marion Albers und Gabriele Britz sein.

Der Autor gibt sich viel Mühe, detailliert die individuellen und überindividuellen, also gesellschaftlichen, Schutzobjekte herauszuarbeiten. In der Zusammenschau schafft er es, die unterschiedlichen Zielsetzungen zu benennen: Schutz vor Publizitätsschäden, von Schamgefühlen, vor enttäuschten Vertraulichkeitserwartungen, Korrespondenz- und Wohnungsschutz, Integritäts- und Identitätsschutz, Schutz vor Profiling und Fremdbestimmung, Kernbereichsschutz, Verhinderung von Diskriminierung, Stigmatisierung und Verhaltenslenkung... Auf gesellschaftlicher Ebene werden als Risiken detektiert Informationsübermacht, Konformitätsdruck, Handelshindernisse.

So rechtswissenschaftlich qualifiziert die dogmatischen Ziselierungen sind, so ignorieren diese die aktuelle bei der Technik ansetzende Schutzzieldiskussion, die mit den Begriffen Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit arbeitet. Diese Schutzziele rechtlich zu vertiefen, wäre wohl eine Doktorarbeit wert.

Erschreckend ist die Realitätssicht des Autors. Zu Beginn seiner Arbeit erdreistet sich der Autor, die Analysen eines Wilhelm Steinmüller in „Fortführung des Klassenkampfes zur Herstellung einer klassen- und autoritätslosen Gesellschaft“ als „postmarxistisch“ und „ideologisch geprägt“ abzutun (S. 10), ohne das zweifellos nicht leicht zu erschließende Hauptwerk von Steinmüller „Informationstechnologie und Gesellschaft – Einführung in die Angewandte Informatik“ (Darmstadt 1993) überhaupt zu erwähnen. Am Ende entpuppt sich der Autor selbst als äußerst ideologisch programmiert, wenn er unvermittelt meint, „die aus dem US-amerikanischen Recht stammende Figur der Vertraulichkeitserwartung (sei) ein brauchbarer Ansatz“ (S. 316). So als traute er sich aber seiner eigenen Chuzpe nicht, beschreibt er kurz und knapp in seinem „Ausblick“ in einem Rundumschlag von Michel Foucault und Jeremy Bentham bis hin zu den „in ihrer Tragweite noch nicht absehbaren Enthüllungen Edward Snowdens“ und der dadurch erkennbaren „Verschmelzung von Staat und Markt“ zu einem „Informationsstaat“, weshalb er mit seinem vorangegangenen auf 300 Seiten beschriebenen kleingerechneten Datenschutz-Einzelschutzzielen doch etwas zu kurz springt (S. 317 f.).

Drackert meint, „bei der Verteuerung oder dem Nichtzustandekommen von Verträgen (handele) es sich nicht um ein datenverarbeitungsrechtliches Risiko, sondern um ein Lebensrisiko“ (S. 314). Was er damit meint, ist offensichtlich sehr analog, etwa, wenn er automatisieerten Scoringverfahren (erst?) dann Eingriffscharakter zuspricht, wenn damit die „Todeswahrscheinlichkeit auf Intensivstationen“ bestimmt wird (S. 308). Informationelle Fremdbestimmung beginnt für ihn (erst?) etwa bei „Erpressungen mit belastbarem Fotomaterial“ (S. 310). Auch wenn er eher zustimmend Kilian zitiert (S. 275), so hat er offensichtlich dessen Grundansatz nicht verstanden, dass gerade personenbezogene Datenverarbeitung im zivilrechtlichen Verständnis einen eigentumsähnlichen Eingriff darstellt, der, wie Eingriffe in das Eigentum, eines umfassenden gesetzlichen Schutzes bedarf. Darum geht es allen Gegnern des Grundrechts auf informationelle Selbstbestimmung: Sie wollen ungestört im kommerziellen Bereich zielgruppenspezifisch vorgehen und hierfür Profiling, Targeting und Marketing praktizieren. Für derartige „normale Marktprozesse“, so Drackert fälschlich, bei denen es um nichts anderes geht, als die „Konsumwünsche der Verbraucher“ zu erkennen, könne man umfassend Art. 12, und 14 GG ins Feld führen. Dies trifft zu einem nicht zu, zum anderen ist zu fragen: Und wo bleibt dann der individuelle Gegengrund Datenschutz (S. 313)? Dass US-IT-Unternehmen mit „normalen Marktprozessen“ unter Missachtung des etablierten Datenschutzes ´zig Milliarden Dollar anhäufen und nicht nur individuelle, sondern ganze Gesellschaften massiv beeinträchtigende Fremdbestimmung betreiben, mag zutreffen, soll aber rechtlich irrelevant sein?

Moderne digitale Grundrechte sind anscheinend nicht nur für Angela Merkel „Neuland“. Umfassend anerkannt sind sie – siehe oben – noch nicht. Dass diese digitalen Grundrechte unserer Informationsgesellschaft sich nicht mit dem Risiko- und Schutzzielkonzept der Industriegesellschaft decken können, sollte sich von selbst verstehen. Richtig ist, dass eine Dissertation, die die Risiko- und Schutzzielrichtungen des „Grundrechts auf informationelle Selbstbestimmung“ und dessen Verzweigungen zu den analogen und den anderen digitalen Grundrechten aufzeigt, noch geschrieben werden muss.

Der Ansatz Drackerts erklärt sich möglicherweise ein wenig damit, dass er die Arbeit in einem Strafrechtsinstitut verfasste. Seine berechtigte Kritik an der „überbordenden strafrechtlichen Rechtsetzung“ und am „überkommenen nationalen Polizeirecht“ (S. 318 f.) kann er aber auf den Datenschutz nicht übertragen. Datenschutzrecht ist nicht „ultima ratio“ und kann es auch nicht sein, sondern ist vielmehr gestaltungsbedürftiges „Informations(verkehrs)recht“.

Die Arbeit liefert nützliches Material, leider aber nicht die richtigen dogmatischen und rechtspolitischen Antworten. Richtig stellt der Autor fest, dass es bisher nur wenige sozial-psychologischen Studien für die zentrale Konformitätsthese des BVerfG gibt. Hier könnte die Forschung zweifellos weitere empirische Erkenntnisse liefern. Dass diese These zutrifft, ist aber nicht nur für Pädagogen und Psychologen, sondern auch insbesondere für (Sicherheits-) Politiker ein Allgemeinplatz.

Jenseits aller dogmatischen Überlegungen überzeugt Drackert auch nicht praktisch: Er bleibt, wie alle Protagonisten der Abschaffung des Gesetzesvorbehaltes im Bereich der Wirtschaft, die Antwort schuldig, wie dies gesetzestechnisch – abgesehen von dem wenig motivierenden Hinheis auf die USA als Vorbild – umgesetzt werden sollte. Es sind gerade die USA, die mit ihrem Schutz von „Information Privacy“ an Inkonsistenz und föderaler Zersplittertheit kaum zu überbieten sind. Dagegen ist das europäische Konzept der Güter- und Interessenabwägung, das nun mal nicht ohne Gesetzesvorbehalt funktionieren kann, geradezu komplexitätsfrei. Auch was die praktische Umsetzung – mit Freiraum lassenden unbestimmten Rechtsbegriffen – angeht, ist Europa überlegen, wenn tatsächlich das Anliegen der Grundrechtsschutz ist. An der Grundrechtsorientierung der von Drackert analysierten Risiken fehlt es. Schade!

Große Qualition:



Gesetz zur anlasslosen Vorratsdatenspeicherung
„Datenhehlerei" ermöglicht Anti-Whistleblower-Gesetz
Unklare Begriffsdefinitionen bei IT-Sicherheitsgesetz
Infragestellung des Prinzips der Datensparsamkeit
Erweiterte Geheimdienstbefugnisse: Artikel 10-Gesetz
Duldung von Geheimverhandlungen bei TTIP

Grafik: Frans Valenta, Bonn